THE ARMY'S COUNTERINTELLIGENCE ROLE IN HOMELAND DEFENSE

A thesis presented to the Faculty of the U.S. Army Command and General Staff College in partial fulfillment of the requirements for the degree

MASTER OF MILITARY ART AND SCIENCE
General Studies

by

FREDERICK L. WASHINGTON, MAJ, USA
Ph.D., Hamilton University, Evanston, Wyoming, 1999

Fort Leavenworth, Kansas
2002

REPORT DOCUMENTATION PAGE

Form Approved OMB No. 0704-0188

1. REPORT DATE (DD-MM-YYYY)	2. REPORT TYPE	3. DATES COVERED (FROM - TO)
31-05-2002	master's thesis	06-08-2001 to 31-05-2002

4. TITLE AND SUBTITLE
THE ARMY?S COUNTERINTELLIGENCE ROLE IN HOMELAND DEFENSE
Unclassified

5a. CONTRACT NUMBER
5b. GRANT NUMBER
5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Washington, Frederick L ;

5d. PROJECT NUMBER
5e. TASK NUMBER
5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME AND ADDRESS
US Army Command and General Staff College
ATTN: ATZL-SWD-GD
1 Reynolds Ave
Ft. Leavenworth, KS66027-1352

8. PERFORMING ORGANIZATION REPORT NUMBER
ATZL-SWD-GD

9. SPONSORING/MONITORING AGENCY NAME AND ADDRESS
,

10. SPONSOR/MONITOR'S ACRONYM(S)
11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
APUBLIC RELEASE
,

13. SUPPLEMENTARY NOTES

14. ABSTRACT

This thesis examines how the Army?s counterintelligence elements currently conduct and could legally increase operations against domestic threats in support of homeland defense. It reviews the joint view of terrorism as the dominant threat to American security and the Army?s view of domestic threat based on current doctrine. This thesis suggests combining joint threat indicators with the threat and criminal categories used by Army counterintelligence and law enforcement. Once combined, a new model would yield a hierarchy of threat groups or criminal categories ranging from terrorist group organizers and supporters to the common criminal. The thesis also examines current legal guidance for conducting counterintelligence in support of domestic operations. Army counterintelligence is usually prohibited from conducting activities that cross into the jurisdiction of the Federal Bureau of Investigation; a few exceptions are allowed to support military operations. When exceptions are allowed, strict parameters are outlined and only for a short duration. With the Army?s increased and continuous role in homeland defense, a review of restrictive procedures is necessary. Research suggest that a need exist for a more definitive and systematic process for conducting such activities. Conclusions and recommendations are provided for improving Army counterintelligence support to homeland defense operations. The objective of this thesis is to provide additional insight toward this goal and generate new concepts and ideas for future research. This thesis examines how the Army?s counterintelligence elements currently conduct and could legally increase operations against domestic threats in support of homeland defense. It reviews the joint view of terrorism as the dominant threat to American security and the Army?s view of domestic threat based on current doctrine. This thesis suggests combining joint threat indicators with the threat and criminal categories used by Army counterintelligence and law enforcement. Once combined, a new model would yield a hierarchy of threat groups or criminal categories ranging from terrorist group organizers and supporters to the common criminal. The thesis also examines current legal guidance for conducting counterintelligence in support of domestic operations. Army counterintelligence is usually prohibited from conducting activities that cross into the jurisdiction of the Federal Bureau of Investigation; a few exceptions are allowed to support military operations. When exceptions are allowed, strict parameters are outlined and only for a short duration. With the Army?s increased and continuous role in homeland defense, a review of restrictive procedures is necessary. Research suggest that a need exist for a more definitive and systematic process for conducting such activities. Conclusions and recommendations are provided for improving Army counterintelligence support to homeland defense operations. The objective of this thesis is to provide additional insight toward this goal and generate new concepts and ideas for future research.

15. SUBJECT TERMS
United States; Army; Counterintelligence; Homeland defense; Homeland Security; terrorism; cooperation; law enforcement; Federal Bureau of Investigation; antiterrorism

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE	Same as Report (SAR)	106	Buker, Kathy kathy.buker@us.army.mil
Unclassified	Unclassified	Unclassified			19b. TELEPHONE NUMBER International Area Code Area Code Telephone Number 913758-3138 DSN 585-3138

MASTER OF MILITARY ART AND SCIENCE

THESIS APPROVAL PAGE

Name of Candidate: MAJ Frederick L. Washington

Thesis Title: The Army's Counterintelligence Role in Homeland Defense

Approved by:

_____, Thesis Committee Chair
MAJ Douglas M. Horton, M.A.

_____, Member
LTC Clay Easterling, M.A.

_____, Member
LtCol Rick J. Messer, B.A.

_____, Member
MAJ Kenneth D. Plowman, Ph.D.

Accepted this 31st day of May 2002 by:

_____, Director, Graduate Degree Programs
Philip J. Brookes, Ph.D.

The opinions and conclusions expressed herein are those of the student author and do not necessarily represent the views of the U.S. Army Command and General Staff College or any governmental agency. (References to this study should include the foregoing statement.)

ABSTRACT

THE ARMY'S COUNTERINTELLIGENCE ROLE IN HOMELAND DEFENSE, by MAJ Frederick L. Washington, 106 pages.

This thesis examines how the Army's counterintelligence elements currently conduct and could legally increase operations against domestic threats in support of homeland defense. It reviews the joint view of terrorism as the dominant threat to American security and the Army's view of domestic threat based on current doctrine. This thesis suggests combining joint threat indicators with the threat and criminal categories used by Army counterintelligence and law enforcement. Once combined, a new model would yield a hierarchy of threat groups or criminal categories ranging from terrorist group organizers and supporters to the common criminal.

The thesis also examines current legal guidance for conducting counterintelligence in support of domestic operations. Army counterintelligence is usually prohibited from conducting activities that cross into the jurisdiction of the Federal Bureau of Investigation; a few exceptions are allowed to support military operations. When exceptions are allowed, strict parameters are outlined and only for a short duration. With the Army's increased and continuous role in homeland defense, a review of restrictive procedures is necessary. Research suggest that a need exist for a more definitive and systematic process for conducting such activities.

Conclusions and recommendations are provided for improving Army counterintelligence support to homeland defense operations. The objective of this thesis is to provide additional insight toward this goal and generate new concepts and ideas for future research.

TABLE OF CONTENTS

LIST OF ILLUSTRATIONS

LIST OF ACRONYMS

AI	Area of Interest
AO	Area of Operation
AR	Army Regulation
CI	Counterintelligence
DA	Department of the Army
DoD	Department of Defense
DTIM	Domestic Threat Intelligence Management
EECI	Essential Elements of Criminal Information
EOC	Emergency Operations Center
FM	Field Manual
FP	Force Protection
INSCOM	Intelligence Security Command
MACOM	Major Army Command
MDMP	Military Decision-Making Process
MI	Military Intelligence
MP	Military Police
OOTW	Operations Other Than War
SASO	Stability and Support Operations
THREATCON	Threat Conditions
TTP	Tactics, Techniques, and Procedures
USACIDC	United States Army Criminal Investigation Command

CHAPTER 1

RESEARCH INTRODUCTION

The United States Army is presently undergoing an important transformation, moving from the Cold War, bypassing the Industrial Age, and attacking the Information Age. Included in this transformation is the integration of intelligence forces at every level. A successful operation requires that intelligence flow seamlessly from national systems to tactical operations within seconds. Figure 1 depicts the intelligence concept for the twenty-first century. This concept is also called Intelligence XXI, the intelligence piece of the evolutionary Force XXI. While considering the changing threats, technological and operational advances, Intelligence XXI simultaneously integrates multi-disciplined intelligence on a non-linear battlefield.

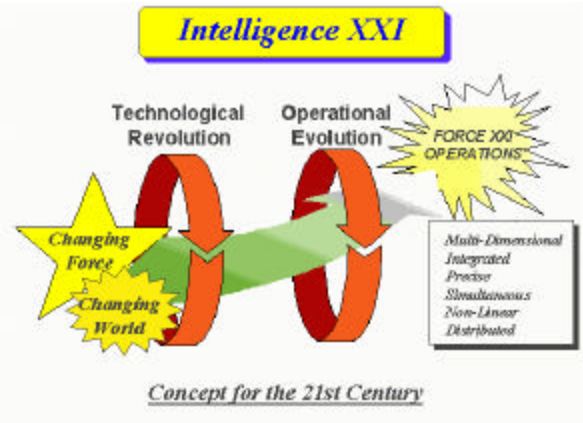

Figure 1. Source: TRADOC Pamphlet 525-75, 1996, figure 2-1.

Under current joint and Army regulations, the procedures used in obtaining intelligence on foreign threats are prohibited on threats that are domestic or American citizen. The topic of homeland defense includes a broad array of missions and mission areas ranging from military assistance to civil authorities to national missile defense. Since the tragedies of 11 September 2001, the topic has attracted a great deal of attention due to the public's heightened awareness of the variety and nature of emerging threats and of the United States' vulnerabilities to them. This thesis investigates how the Army's intelligence elements should legally conduct operations against domestic threats in support of homeland defense from a strategic perspective. This perspective places homeland defense missions within the larger spectrum of operations. In so doing, it exposes potential problem areas--missions requiring more or a different force structure than that already available--for further action by the Army.

Military requirements to support security strategy prompted an increase in antiterrorism and counterthreat initiatives. This condition placed new requirements on the Department of Defense (DoD) and the United States Army to continuously evaluate threat and vulnerabilities and to establish viable countermeasures to mitigate potential risks.

Problem Background

The Army's counterintelligence role in homeland defense operations is an inclusive, intricate, and resource intensive mission. It involves the continued management of counterintelligence operation against foreign threats and the evolution of management for domestic threats within the continental United States (CONUS) and its territories. Recent terrorist attacks revealed numerous gaps in protecting the homeland.

Additional requirements were identified without the immediate allocation of additional resources.

Army counterintelligence elements must develop new procedures to accommodate an assortment of issues. They must decipher the complex legal implications associated with collecting intelligence in a domestic environment, possibly against US citizens. This will also require the development of new or improvements of current intelligence networks with the other services, military police, federal, state, and local law enforcement agencies in support of homeland defense. This also requires procedures for ensuring detailed coordination with the Office of the Judge Advocate General (OTJAG) and procedures for determining and monitoring legal liability against homeland defense restrictions.

New procedures to identify intelligence gaps are required. Army intelligence officials must develop a thorough understanding of how they support this new area of responsibility. This means Army intelligence must provide sanitized products and disseminated them to various civilian agencies. These products must provide a clear picture of potential threats at the local level, and simultaneously provide a formal and standard product for the national intelligence community.

Although the Director of Central Intelligence (located in the center of the wheel in figure 2) has the responsibility for coordinating the overall intelligence effort for the US, the Director of the Federal Bureau of Investigation has responsibility for coordination of domestic intelligence. Eight of the thirteen agencies making up the National Intelligence Community are military organizations. The remaining five organizations have military elements assigned as liaisons.

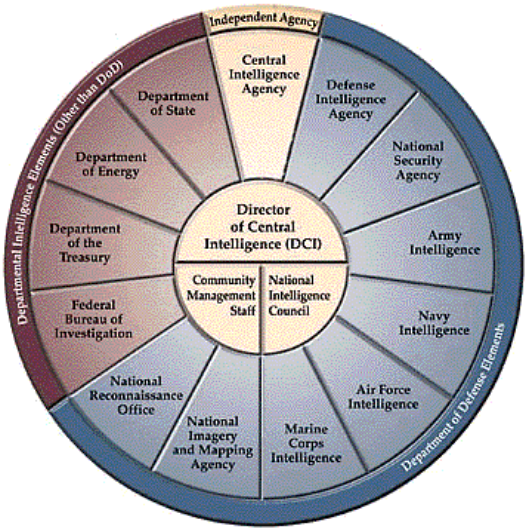

Figure 2. United States Intelligence Community. Source: CIA 2002.

The Army's increased involvement in low-leveled interventions and peace operations has placed new emphasis on reducing criminal activity as a required part of stabilizing an area of operations. In response, the Military Police Corps added the new mission of police intelligence operations. This created the requirement to develop and publish new policies and procedures for managing threat intelligence.

Along the same lines of developing new doctrine, missions, or regulatory guidance, Army intelligence officials will need time and resources to determine the number of challenges affecting counterintelligence support to homeland defense operations. A broad comprehensive review of current practices, an assessment of success and shortcomings, and the development of guidance based on findings will determine progress. At best, this process will be evolutionary characterized by incremental improvements. The development of proposals for future adoption must include a

thorough examination of the current counterintelligence features of supporting homeland defense operations. While implementing incremental improvements, each step toward improving Army counterintelligence support to homeland defense must consider the previous step before designing the next. Hopefully, this thesis represents one such step.

Primary Question

How should Army's counterintelligence elements legally increase operations against domestic threats in support of homeland defense?

Related Subordinate Questions

1. How will the Army assess and categorize threats to homeland defense?
2. How should homeland defense be defined?
3. Which liabilities or restriction must change for Army counterintelligence elements to effectively support homeland defense?
4. Will the absence of Army counterintelligence adversely affect the Army's ability to support homeland defense operations?

Answering the primary question will have important application to Army operations, employment, training, and doctrine. Answering the secondary questions will provide a foundation, which leads to future research and development

Background

Limitations of Military Use in Domestic-Civil Intervention

One strategic role shared by the Department of the Army (DA), along with other DoD members, is to defend the population and homeland. When necessary, the Army can defend against a foreign military force, threat, or invasion. When internal threats are

considered beyond the capability of civil authorities, the Army can defend against them also. Defense against internal threats, as it pertains to enforcing civil laws, is severely restricted by the Constitution, US law (Posse Comitatus Act of 1878), and American traditions dating back to the post-Civil War restoration period (FM 100-19 1993,3-0). However, "there are two constitutional exceptions, based on the legal right of the United States to guarantee the preservation of public order and the carrying out of governmental operations . . . by force if necessary" (Gilligan 1999, 4). The first exception is granted by "emergency authority," which permits the use of the Army in situations when "civil disturbances, disasters, or calamities, seriously endanger life and property and disrupt normal governmental functions" (Gilligan 1999, 14). The second exception grants the Army with the right to protect federal property and military functions (Army missions):

> The right of the United States to protect federal property or functions by intervention with federal military forces is an accepted principle of our government. The right extends to all federal property and functions wherever located. This form of intervention is warranted, however, only where the need for protection exists and local civil authorities cannot or will not give adequate protection (Title 5, *US Code*, 1998, vol. 301).

There are two "common law" exceptions to consider. The first allows a military member to act as private citizen in defending against internal threats or otherwise supporting civil authority. This parallels other rights retained by a military member when acting as a private citizen, notwithstanding his military status (Gilligan 1999, 35). The second exception is included under "Military Purpose Doctrine" and allows the Army the ability to assist civil authorities in pursuit of a military purpose, when any benefit to civil authorities is only incidental. An example here might involve the use of MP explosive-detector dogs at an off-post church attended by military family members. The purpose is

to protect military family members, but the reality is that it also protects community members and nonmilitary property is an incidental benefit to local civil authorities.

The Army's right and responsibility to defend against internal threats based on the constitutional exception to "protect federal property and functions," and the common law exception to assist civil authorities to achieve a "military purpose" are probably the most important and the least understood of these four exceptions. These exceptions grant generous latitude to establish security on CONUS installations, but the interpretation of such permissions off of the installation is confusing. These exceptions may provide some important avenues for granting the Army the ability to influence the threat environment beyond the installation's borders.

Mission to Protect United States Interest

"Title 10, *US Code (USC)* requires the Army to issue regulations for the safety of its people and the preservation of its property" (O'Hanlon, 2000, 11-17). While the nature of domestic security is yet underdeveloped, this means that the Army has an inherent responsibility for providing defense of the continental US (CONUS) and its territories. The responsibility for implementing these regulations is normally delegated to installations, but can easily flow to every element or echelon responsible for personnel, information, and critical resources. By the end of the last decade, installation security had become the focus of Joint Service Installation Vulnerability Assessment teams. These teams worked with commanders and staff to assess baseline compliance, to document new developments, and to educate commanders and their staff.

The minimum requirement for security should be to safeguard persons assigned or visiting the installation, protect critical resources, sustain mission objectives, and secure

military information. Responsibilities may include protecting classified information, securing weapons, interdicting drug trafficking, or any even include highly specialized missions, such as security support for the US president, US and foreign dignitaries, or other high-ranking military officials meeting or visiting in or around the installation or within its specified jurisdiction.

Local threat conditions may dictate additional security responsibilities for installation commanders and their staff. The installation staff must assess the effect of local threat conditions on the security of the installation to determine the appropriate requirements. As a minimum, the assessment should consider three factors: (1) the effects of local threat to installation interests, (2) missions or contingency plans supported by the installation, and (3) the unique "target value" of force protection objects associated with the installation. (Target value is not a doctrinal term; however, it refers to the specific incentive value that a particular installation, activity, person, or information may present to a criminal or criminal organization, whether it is of symbolic value, monetary, recruitment, prestige, or power.)

Local threat assessment usually provides a threat picture specific to a single installation or grouping of installations based on the threat factors mentioned above. This means that each installation may have specific security requirements tailored to its individual assessment. (Two exceptions to this specificity were the 1998 force protection mandate requiring all CONUS installations to establish threat condition (THREATCON) A-plus status, in response to terrorist on American Embassies in Africa and immediately following the terrorist attacks on 11 September 2001, when all US military installations implemented TREATCON D.) As assessments are updated, security requirements

continue to change to reflect the change in threat conditions. This constant change acts to reinforce installation specificity and as a result, has diminished initiatives toward standardizing threat countermeasures, except in the broadest sense, such as those found under published THREATCON. But even THREATCON measures can be tailored to address unique security requirements, such as blending particular measures from THREATCONs A and B to arrive at A-plus as illustrated in the example above.

Using Intelligence for Security and Force Protection

The shifting nature of threat conditions requires an organization's staff to plan, prepare, and prioritize countermeasures. Understanding the threat environment at all three levels of war: strategic, operational, and tactical is critical. Conceptualizing a picture of global security concerns and threats against domestic interest, threats to the Army, and threat evolving from the local environment is the first step to developing countermeasures. Followed by careful consideration of the security resources and external support available. This leads to selection of the appropriate security task and implementation of the necessary measures to counter threats against critical resources, personnel, and information. With a clear understanding of the intent, type, and capabilities of the threat, an effectively plan can implement countermeasures without imposing undo burdens on the service provider and customer. Regardless, the value of the countermeasure must be compared to the benefits gained.

A vital role in this process is Intelligence. As identified in the *Military Requirements of the Defense Strategy:* "Because intelligence represents the first line of defense, DoD has implemented procedures to improve its collection and use of terrorism-related intelligence, getting the needed product into the hands of local commanders as

rapidly as possible"(Rumsfeld 1998, 8-9). It allows leaders to develop a clear picture of potential threats against their interest and apply appropriate countermeasures. Based on this, leaders are able to improve their programs by refining security processes through improved security planning, security and response training, resource economy, and crisis management.

Resource economy is probably the most important factor. Intelligence can help to economize resources by limiting false responses, allowing resource sharing among agencies, and minimizing strategic consumption. There are a number of ways intelligence can help to prioritize the security workload. First, by directing security toward actual threats, this can ensure that an agency reacts to the threat with the appropriate response, and avoids implementing countermeasures against nonexistent threats. Second, it allows leaders to counter the most dangerous threat, minimize the lesser threat, and accept risk associated with the negligible threats. Finally, intelligence can confirm the absence of threat, allowing agencies to share resources when and where appropriate.

Defining Counterintelligence in Support of Homeland Defense

Army counterintelligence authority is derived from:

1. Executive Order 12333, United States Intelligence Activities
2. 10 USC 164 and 3033 (Public Law 99-433, Goldwater-Nichols Department of Defense Reorganization Act of 1986)
3. 18 USC 801-940, The Uniform Code of Military Justice (UCMJ)
4. 50 USC 401, et seq., The National Security Act of 1947
5. 50 USC 1801, et seq., The Foreign Intelligence Surveillance Act of 1978

6. Public Law 100-180, Defense Authorization Act for Fiscal Year 1988 and 1989

7. Agreement Governing the Conduct of Defense Department Counterintelligence Activities in Conjunction with the Federal Bureau of Investigation (FBI) copyright, 5 April 1979; and supplement (S), 20 June 1996

8. (U) Attorney General Guidelines for FBI Supervision or Conduct of Espionage Investigations of US Diplomatic Missions Personnel Abroad, 17 April 1990

9. (U) DoD Directive (DoDD) 5210.48, DoD Polygraph Program

10. (U) DoDD 5240.2, DoD Counterintelligence

11. (U) DoD Instruction (DoDI) 5240.4, Reporting of Counterintelligence and Criminal Violations

12. DoDD 5240.6, Counterintelligence Awareness and Briefing Program

13. DoDI C-5240.8, Security Classification Guide for Information Concerning the DOD Counterintelligence Program (U)

14. DoDI S-5240.9 (S), Support to Department of Defense Offensive Counterintelligence Operations (U)

15. DoDI 5240.10, DOD Counterintelligence Support to Unified and Specific

The Army's counterintelligence elements will conduct aggressive and coordinated investigation, operations, collection, analysis and production, and other counterintelligence services worldwide. The purpose of Army counterintelligence is to counter foreign intelligence, terrorist, adversary, and entity collection efforts and activities. Additionally, Army counterintelligence attempts to prevent sabotage, subversion, sedition, foreign assassination efforts, and other foreign threats. Army

counterintelligence conducts these activities to protect DA or DoD soldiers, civilians, contractors, family members, operations, installations, equipment, information, technologies, and activities. Counterintelligence agents will plan and execute all counterintelligence functions in accordance with the authorities listed above. This mission and the regulations and directives governing counterintelligence activities apply during peacetime as well as all levels of conflict. The Army counterintelligence force will concentrate its effort in three primary mission areas: counterintelligence support to force protection, counterintelligence support to technology protection, and counterintelligence support to infrastructure protection.

Counterintelligence Support to Force Protection

Force protection is the responsibility of commanders at all levels. Virtually every discipline and skill set in the Army contributes to force protection. Counterintelligence contributes to the overall force protection effort by conducting collection investigations and operations to determine foreign activities which threaten the survivability and mission accomplishment of Army soldiers, civilians, and units and then provides counterintelligence analysis, production, and other counterintelligence services to counter this threat. In the past, counterintelligence support to force protection was primarily focused outside the CONUS on foreign personnel and installations, but recent terrorist threats and attacks caused the expansion of this mission area to include vigorous counterintelligence support in CONUS and to units in transit. The homeland defense mission is still in development but is an extension of force protection. Every function of Army counterintelligence will be vigorously exercised in support of homeland defense and force protection.

Counterintelligence Support to Technology Protection

Counterintelligence has provided support to technology protection for many years under counterintelligence support to special access programs (SAP) and will continue to do so. Over the last ten years, counterintelligence support to technology protection has grown rapidly to cover key developing technologies that support Army transformation. The purpose of counterintelligence support to technology protection is to preserve the Army's technological advantage. Counterintelligence support to technology protection includes the use of technology, not just the technology itself and is conducted in the same way as counterintelligence support to the protection of information, personnel, and units. Counterintelligence will:

1. Assess the threat to the technology, lab, test center, or acquisition program
2. Educate the Army personnel and units in contact with the technology, organization, facility, or installation
3. Conduct investigation, collection, and operations to counter foreign attempts to gain access to the technology
4. Provide analysis, production, and other services in a continuing cycle of activity.

Counterintelligence Support to Infrastructure Protection

Counterintelligence support to infrastructure protection is defined in two distinct ways and Army counterintelligence will support both. Until recently, counterintelligence support to infrastructure protection referred to information systems infrastructure and databases. In this role, Army counterintelligence works in close coordination with the US Army Criminal Investigations Command (USACIDC) to provide a rapid investigative

capability in response to intrusions to Army and DoD computer systems and databases. Counterintelligence will work in close coordination with CID until the intrusion is determined to be a criminal or foreign intelligence, entity, or terrorist nature. If it is determined that the intrusion is criminal in nature, USACIDC will investigate unilaterally. If it is determined to be of a foreign intelligence, entity, or terrorist nature, Army counterintelligence will have primacy over the investigation. Because of the War on Terrorism and homeland defense, infrastructure protection is now also defined as the protection of any critical infrastructure from power grids to water supplies. Counter-intelligence support to infrastructure protection will be conducted as it is in force protection to ensure survivability and mission accomplishment.

Intelligence in support of homeland defense involves collecting, processing, disseminating, and storing threat intelligence as it relates to the defense of the United States and its territories and with respect to legal parameters. This definition provides a direct approach to the application of homeland defense. Three important points are worth highlighting: (1) threat is associated with crime and not other accident, incidents, or natural disaster; (2) for intelligence processes relating to the military, threats must pertain to DoD interests; and (3) threats must affect those interest affecting the continental US or its territories. The first point establishes the connection between threats and criminal activities or conditions. This linkage helps to broaden the scope of threat intelligence from a more traditional focus on conventional adversary or special purpose forces, to include a full range of "threat groups" comprised of seven categories: terrorist, saboteurs, organized criminals, unsophisticated criminals, drug traffickers, gangs and hate groups, and extremists. Chapter 4 outlines this important distinction.

The second and third points are the foundation for the current status and challenges confronting intelligence operations in support of homeland defense. The military is severely limited to conducting intelligence against US citizens in a domestic environment. This limitation derives from DoD Regulation 5200.27, *Acquisition of Information Concerning Persons and Organizations Not Affiliated with the Department of Defense,* and precludes military intelligence elements or organizations from conducting intelligence operations targeting US citizens (NAIC 2000, 3). This limitation severely restricts military intelligence element's ability to provide threat intelligence in support of homeland defense. Although military intelligence elements and organization may provide or share intelligence linking foreign threats against domestic targets or any intelligence relating to members of the military community, it is strictly prohibited from conducting intelligence operations regarding domestic threats originating outside military installations.

Research Outline

The research outline consists of three sections as outlined below. Each section includes discussions based on research and experience concerning potential gaps in homeland defense. The first two sections focus on how the Army views and determines threats to homeland defense and on what the legal considerations are in conducting intelligence against such threats. Realizing the Army does not engage in operations in the absence of intelligence, the third section discusses current intelligence initiatives and possible intelligence operations, which might be performed, based on the conclusions from the first two sections.

Section I. Determining Threat

This section includes a discussion of the Army's view of terrorism, its emphasis on terrorism as the primary threat, and the current method for determining the threat level. It discusses both international and domestic terrorism. Should these types of terrorist be treated differently? This section will propose an answer and offer a potential solution to determining the threat.

In determining the threat, Army counterintelligence may have to rely on law enforcement procedures to assist in identifying this large category of offenders. This section also discusses six additional criminal categories or threat groups and presents a more balanced view with respect to the "worst versus most likely scenario" of potential domestic threats. Finally, this section covers current methodology for determining terrorist threat levels and proposes a new model for determining threat across the broad spectrum of threat groups.

Section II. Defining Legal Parameters for Intelligence Support to Homeland Defense

This section provides the legal implications of conducting counterintelligence in support of homeland defense operations. This area has the greatest impact on homeland defense but is yet an underdeveloped area. Counterintelligence will often pass leads, parallel, and support the efforts of law enforcement. The second section reviews the legal implications of conducting counterintelligence against domestic threats in support of homeland defense. Although no case law or precedence was discovered in this area, similar examples were located where the court system interpreted the parameters of military law enforcement with respect to US citizens on a case-by-case basis. Once

applied to current law and regulatory guidance, appellate decisions can provide key insights that may expand, contract, or maintain the status quo of current counter-intelligence and military law enforcement processes. Regardless of case outcome, court findings provide an ever-changing process for evaluating, assessing, and adjusting current regulations governing the legal conduct of counterintelligence in support of domestic law enforcement or homeland defense.

Although a review of several appellate cases revealed only a negligible impact on homeland defense operations, an impact, nevertheless, may exist based on the relationship between homeland defense and domestic law enforcement. Since homeland defense parameters parallel those of domestic law enforcement, any progress in one field should relate to the other. This premise is bolstered by a few examples of recent appellate decisions that may indirectly affect the legal guidelines for conducting intelligence operations against domestic threats in support of homeland defense. Finally, this section reviews current legal parameters for conducting counterintelligence operations against domestic threats and proposes a new model for determining a military link to the offender. This model suggests a systematic process for organizing and prioritizing essential elements to determine a military connection. It also provides measurement for evaluating the potential legal liability involved with domestic operations.

Section III. Conducting Counterintelligence Operations in Homeland Defense

This section includes some of the most recent initiatives to refine threat intelligence in homeland defense. This cursory review, covers current progress in

standardizing and improving homeland defense processes. While Army counterintelligence and USACIDC's missions and methods are significantly different, their efforts intersect in the homeland defense arena. This section highlights the USACIDC's "Domestic Threat Intelligence Management Model (DTIM)," which represents an important contribution in this effort. The model portrays DTIM as a continuous cycle, organized into four phases: (1) Intelligence Collection to identify threat, provide advance warning, and disseminate threat intelligence; (2) Threat vulnerability Assessment to measure potential strengths and weaknesses in installation defenses; (3) Crisis Management, which relies on real-time intelligence for incident response and mitigation; and (4) Analysis and Deterrence, which uses intelligence for investigating, reporting, and capturing lessons learned. This section also discusses essential intelligence, law enforcement, security, and agencies involved in this process.

Limitations

The largest constraint with this topic is the lack of recent published literature covering the Army's counterintelligence role in homeland defense. There are several publications covering federal, state, and local government roles and concerns in homeland defense but very few focuses on the specific roles or challenges facing the Army. This restraint is central to the thesis and requires a great deal of attention in answering the primary and secondary questions.

Delimitations

This thesis will not address the analysis of intelligence or information relating to homeland defense but rather assumes the analysis is parallel to civilian agencies. Also

this thesis will not attempt to provide a definitive echelon or agency to be responsible within the Army, but it will focus on the areas that may present a particular challenge in supporting homeland defense, in an attempt to provide insight and general guidance. This study will not separate or address the role of the National Guard as opposed to the Active Army.

Assumptions

This thesis makes two fundamental assumptions. First, the US will remain engaged throughout the world for the foreseeable future. As a result, its national security strategy of "Engagement" and its national military strategy of "Shape, Respond, Prepare Now" will remain unchanged in principle, even if the terms and priorities are altered (Zoellick 2000, 45). Second, if US national culture and historical traditions are any indication, Americans will demand a domestic environment in which their homeland is secure. Accordingly, the US military will perform the bulk of its homeland defense missions as the supporting rather than the lead federal agency and may have to comply with fairly restrictive rules of engagement (Lujan 1996, 82)

Definition of Homeland Defense, Mission Areas, and Terms Used

The US government needs to develop a comprehensive definition of homeland defense to provide a uniform basis for coordinating the efforts of all federal agencies and for deriving mission areas, tasks, and responsibilities for each. Remarkably, however, homeland defense has not yet been authoritatively defined, either at the interagency level or by the defense community. Part of the reason for this is the disagreement over whether the definition should address only the requirement to "deter and defend against

foreign and domestic threats" or whether it should encompass "all hazards," including natural and man-made disasters. Some views, such as those offered by RAND Arroyo, favor the former--a more circumscribed definition--because it provides a clear distinction between "military activities" and the "activities of civilian organizations" (Peters 2001, 71). They argue that such distinctions will reduce damage to the military's image, which could suffer harm if it is perceived as doing either too little or too much.

Unfortunately, definitional clarity will not necessarily preclude misperceptions of whether the military has actually done too little or too much in any particular homeland defense situation. Furthermore, a circumscribed definition tends to make the problem fit the tools available and thus would not help expose potential organizational or procedural weaknesses in the ways the US Government and the joint community proposes to protect the homeland. In the absence of an authoritative definition, the Army has rightly developed and tentatively approved the following "all-hazards" definition in its homeland defense*: Strategic Planning Guidance* (draft dated 8 January 2001). "Homeland Defense is protecting our territory, population, and infrastructure at home by deterring, defending against, and mitigating the effects of all threats to US sovereignty; supporting civil authorities in crisis and consequence management; and helping to ensure the availability, integrity, survivability, and adequacy of critical national assets." Such a definition avoids dividing national security into "domestic" and "overseas" concerns and thereby helps preserve unity of effort in the execution of the national security and national military strategies. Second, it assists in reducing the potentially disruptive impact of an incident in which it is not clear whether hostile intent is involved by enabling the creation of a

single chain of command appropriate for either situation. Finally, it facilitates the establishment of priorities and the allocation of resources.

Definition of Terms Used

Key to this study is understanding the following terms as defined:

Antiterrorism includes defensive measures used to reduce the vulnerability of individuals and property to terrorist attacks, to include limited response and containment by local military forces. Antiterrorism is a consideration for all forces during all types of military operations. Commanders take the security measures necessary to accomplish the mission and protect the force against terrorism. Soldiers are often most vulnerable during off-duty periods and in the recreational locations. Soldiers and families that reside outside protected installations are ideal targets for terrorists. Commanders make every reasonable effort to minimize the vulnerability of their force to hostage taking. Typical antiterrorism actions include: coordinating with local law enforcement; positioning and hardening of facilities; taking physical security actions designed to prevent unauthorized access or approach to facilities; taking crime prevention and physical security actions that prevent theft of weapons, munitions, identification cards, and other materials; establishing policies regarding travel, size of convoys, breaking of routines, host-nation interaction, and off-duty restrictions; and providing for protection from weapons of mass destruction (FM 3-0, 2001, 9-12).

Counterterrorism is the offensive measure taken to prevent, deter, and respond to terrorism. Army forces participate in the full array of counterterrorism actions, including strikes and raids against terrorist organizations and facilities outside the US and its territories. Counterterrorism is a specified mission for selected special operations forces

that operate under the direct control of the National Command Authority (NCA) or under a combatant command arrangement. Commanders who employ conventional forces against organized terrorist forces operating in the area of operation (AO) are conducting conventional offensive operations, not counterterrorism operations (FM 3-0, 2001, 9-11).

Commander's Force Protection Critical Tasks. A comprehensive list of requirements identified by the commander as being critical in facilitating timely force protection management and the decision making process that affect successful force protection accomplishment (see figure 3).

Criminal Intelligence. The product(s) that result from the collection, analysis, and interpretation of all available information concerning known and potential criminal threats and vulnerabilities of supported organizations.

Domestic Threat. Terrorist or criminal threat perpetrated by the citizens of one country against fellow countrymen. That includes acts against citizens of a second country when they are in the host country, and not the principal or intended target.

Domestic Threat Intelligence. Intelligence relating to criminals, crimes, or activities or conditions within the US that pose a threat to internal security.

Domestic Threat Intelligence Management (DTIM). Established procedures for managing information collection and intelligence processing, dissemination, and storage.

Domestic Threat Intelligence Management Model. A USACIDC model that synchronizes intelligence management through four phases of USACIDI force protection support, including: threat assessment, vulnerability assessment, crisis management, and analysis and deterrence.

Force Protection. Security program designed to protect service members, civilian employees, family members, facilities, and equipment in all locations and situations, accomplished through planned and integrated application of combating terrorism, physical security, operations security, personal protective services, and supported by intelligence, counterintelligence, and other security programs.

Forced Protection Objects. The potential target of terrorist attack (i.e., personnel, critical assets, or information).

Forced Protection Program Elements. Subprograms of force protection designed to protect FP objects (i.e., personnel security, physical security, law enforcement, and information operations). Program elements are supported by the synchronization of doctrine, training, operations, intelligence, and resources.

Intelligence. The product resulting from the collection, processing, integration, analysis, evaluation, and interpretation of available information.

Joint Services Integrated Installation Vulnerability Assessments (JSIVA) Team. A team under the Defense Threat Reduction Agency (DTRA) charged with providing independent assessment capabilities to the CINCs, services, and agency directors, along with technical expertise and assistance in meeting force protection standards. This team provides installation commanders on-site assessments by examining the vulnerabilities to potential terrorist attack and other threats within its area of responsibility.

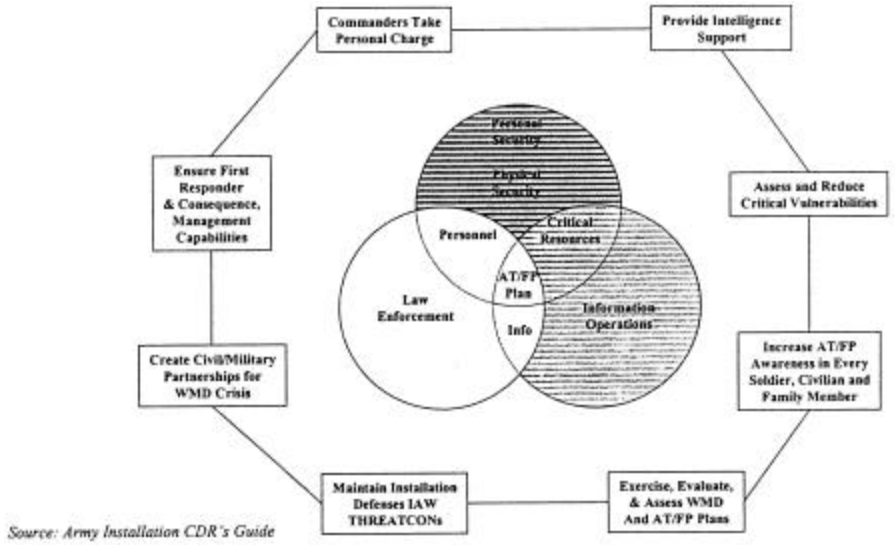

Figure 3. Force Protection Doctrine, Installation Commanders' Antiterrorism Guide. Source: JP 3-07.2, 1998, 2-8.

Posse Comitatus Act of 1878, 18 *US Code,* Statue 1835, a criminal statue which prohibits the use of the military to enforce civilian laws.

Terrorism is the calculated use of unlawful violence or threat of unlawful violence to inculcate fear. It is intended to coerce or intimidate governments or societies. Terrorists usually pursue political, religious, or ideological goals (FM 3-0 2001, 9-11). Enemies who cannot match an adversary's conventional force often turn to terrorist tactics. Terrorist attacks often create a disproportionate effect on even the most capable conventional forces. Terrorist tactics include: arson, hijacking, maiming, seizure, assassination, raids and ambushes, sabotage, hoaxes, bombing, kidnapping, hostage taking, and employing weapons of mass destruction. Army forces routinely conduct operations to deter and defeat these attacks.

Threat Conditions

There are four threat conditions (THREATCONs) above normal:

1. THREATCON ALPHA: This condition applies when there is a general threat of possible terrorist activity against personnel and facilities, the nature and extent of which are unpredictable, and circumstances do not justify full implementation of THREATCON BRAVO measures. The measures n this THREATCON must be capable of being maintained indefinitely.

2. THREATCON BRAVO: This condition applies when an increased and more predictable threat of terrorist activity exists. The measures in this THREATCON must be capable of being maintained for weeks without causing undue hardship, affecting operational capability, and aggravating relations with local authorities.

3. THREATCON CHARLIE: This condition applies when an incident occurs or intelligence is received indicting some form of terrorist action against personnel or facilities and is imminent. Implementation of measures in this THREATCON for more than a short period probably will create hardship and affect the peacetime activities of the unit and its personnel.

4. THREATCON DELTA: This condition applies in the immediate area where a terrorist attack has occurred or when intelligence has been received that terrorist action against a specific location or person is likely.

CHAPTER 2

LITERATURE REVIEW

Introduction

The primary purpose of this chapter is to provide a review of the literature relating to the Army's counterintelligence role in homeland defense operations. This chapter examines the patterns of literature that have emerged in the last four decades to expand and limit homeland defense. It includes some milestones that have caused institutional pressures for providing homeland defense-related services, but also addresses the lack of supporting literature for providing "how to" systems and processes. This chapter discusses the growing trend in Army literature leading to the generalization of threat and an opposing trend by joint doctrine toward a specific characterization. It will include a look at doctrine that pertains to threat within the domestic environment and those operations countering the threat in external environments. Finally, it reviews USACIDC's latest attempt to address the issues in its publication of Operations Memorandum 002-00*, Force Protection Initiatives and Domestic Threat Intelligence Management in early 2000* (USACIDC 2000, 3).

Very little has been published that covers the Army's counterintelligence role in homeland defense; however, there are several literary categories that cover related areas and parallel certain aspects of homeland defense operations. Most of these sources require interpretation to identify their relationship to homeland defense, some of the observations will require broad generalizations, and a couple will require a stretch of the imagination. Regardless of this limitation, there is enough information to base a foundation for homeland defense.

This topic is of importance for the following reasons: (1) This topic will serve to heighten the awareness of policy makers and decision makers. The Army's doctrine and policies are based on success and lessons learned and after-action reviews from operations. A threat organization will conduct its own after-action review and develop methods to counter the US's success. (2) This topic will enlighten and hopefully help to protect America's most valuable resources, the citizens and soldiers. (3) This topic can assist in balancing the focus of roles for Army counterintelligence personnel in support of domestic missions. And (4) this topic will explore the necessity for governmental agencies to expeditiously share information internally and externally.

Influence of the Media and Politics

Numerous strategic-level defense, security, or military document includes an important topic related to homeland defense. The *National Security Strategy for a New Century, the National Defense Strategy, the National Military Strategy,* the *United States Army Posture Statement FY01, Quadrennial Defense Review,* and a host of other parallel or supporting documents are in this category. There are topics in these sources focusing on threats or threat effects against the domestic environment. The most prevalent buzzwords and phrases are: homeland defense, transnational threats, terrorism, drug trafficking, international crime, domestic preparedness, and weapons of mass destruction. The main point of their messages is essentially the same: internal and external threat groups are in the rise, their capabilities are advanced, and they will leverage technology and destructive weapons to gain asymmetry. This passage from *A National Security Strategy for a New Century* provides an example of these literature sources:

> Our potential enemies, whether nations or terrorists, may be more likely in the future to attack against vulnerable civilian targets in the United States. At the same time, easier access to sophisticated technology means that the destructive power available to rogue nations and terrorists is greater than ever (White House 1999, 15).

These documents provide the source for the military's emphasis on domestic threat. As such, these political-military documents provide the incentive for Army counterintelligence in support of homeland defense, to include both, potential support to civil authorities and domestic US Army interest. Several sources refer to the need to increase intelligence capabilities, for most it is an implied task. Accordingly, within the documents mentioned above, any reference to conducting counterintelligence operations against a domestic threat remains general or unspoken.

Congress has also hosted a number of heated debates on topics related to or with emphasis on domestic security. The media continues to display the military's role, with respect to the implications of laws and traditions limiting its involvement in civil affairs. Numerous articles have documented this controversy, especially during times of or associated with domestic threat or terrorist incidents, such as the Oklahoma City bombing, the attack on the USS *Cole,* World Trade Center, or Pentagon. Media stories provide a good sensing of the level of interest and sensitivity to domestic threat, identify failures to counter domestic threats, and cover political trends. However, the effect of the media on civil-military cooperation and, specifically, reporting on intelligence operations, are beyond the scope of this research, and therefore media articles included in this study are only cited with reference to their content.

Prior Research

The second category addressed is prior research. As presented in chapter 1 as an anticipated problem, limited sources were available. No sources, Internet sites, or subject matter experts were discovered that specifically addressed the Army's intelligence role in support of homeland defense. From the law enforcement perspective, the closest related source was a published memorandum by Criminal Investigation (CID) that presented the domestic threat intelligence model (DTIM) operations within the Army. Unfortunately, the application of military threat intelligence in the domestic environment has been predominately an informal process.

Indirect sources are introduced and discussed as they generally relate to certain aspects of homeland defense. Because of the controversy often associated with the speculative nature of indirect sources, a discussion of these categories in this chapter and subsequent ones will attempt to develop the relationship between parallel or associated research. Discussions will endeavor to avoid confusing concepts or terminology. Instead, discussions will use existing terms and principles where applicable, clearly establish the premise for necessary modifications, or address the more complex interpretations (stretching the imagination).

The most current information available will be used to identify newly created principles or terms. In the absence of guidance in the way of domestic threat intelligence, it is important not to violate any standing principles, terms, or "how to" methodology, without due explanation and consideration. Unless making a connection between this thesis and a related topic, regulations, field manual (FM), and policies will be utilized

within their stated parameters, be it intelligence, law enforcement, force protection, or other related topics.

Threat Doctrine

The third category of literature is threat doctrine. This primarily includes the two separate concepts offered by joint and Army doctrine. Relating to threat, Army doctrine can be further subdivided into "administrative" and "operational" literature. The contrast among these classifications simply separates threat literature by its relationship with Army operations or by its relationship with administrative programs. Operational literature covers those threats that are discussed as a part of doctrine associated with small wars, operations other than war (OOTW), peace operations, stability operations, support operations, and several other types. On the other hand, administrative threat literature covers Army programs or program requirements with respect to threat guidance, operations, and policies. This includes force protection, security, physical security, loss prevention, crime prevention, and numerous others programs countering a threat.

The distinction between operational and administrative literature touches on semantics, but it has some important considerations when researching the question of threat. As discussed in chapter 4, in the analysis of Army threat doctrine in chapter 4, this distinction is important in recognizing and understanding the effects of recent trends in Army doctrine to merge these two separate classifications. Prior to the publication of FM 100-5 *Operations*, and FM 3-0, operational doctrine primarily focused on one enemy or opposing forces, it has more recently been forced to consider a much larger array of threats.

With the exception of opposing forces at the high end of the spectrum of conflict, the recent trend in Army doctrine seems to embrace all threats in a catchall fashion. At the lower end of the spectrum, doctrine recommends planning and preparation against a vast possibility of treats. The theoretical implications of this include redundant, generalized, and unstructured threat doctrine, instead of creating a useful model, such as that used for calculating combat power relative to the well-defined threat from an opposing force. Commanders and staffs must now contend with a shapeless variety of threats opposing Army interests. This leads to contingency planning against several threat definitions or descriptions from a variety of sources that are often open for interpretation, confusing, or general in nature.

The real-world implications of this trend are that commanders and staffs must sort through a complex picture of threat and decipher from it, something meaningful within the specific context of their own environment

Similar to Army doctrine, joint doctrine is concerned with the threat presented by asymmetric effects. Joint doctrine, selectively fielded more specific doctrines that combine both administrative and operational threat doctrine under the same jacket. An example is JP 3-0.7.2, *Joint Tactics, Techniques, and Procedures for Antiterrorism*, it consolidates antiterrorism as an aspect of both administrative and operational doctrine. It has some of the requirements of a program, it develops the subject as an operational consideration. Other publications that focus on this type of asymmetric threat is also included in the following publications:

1. JP 3-07, *Joint Doctrine for Military Operation Other Than War*

2. JP 3-07.7, Joint Tactics, Technique, and Procedures for Domestic Support Operations

3. JP 3-10.1, *Joint Tactics, Technique, and Procedures for Base Defense*

4. JP 3-54, *Joint Doctrine for Operations Security*

In joint doctrine, the most visible trend is its focus on terrorist as the primary threat in a domestic environment and certainly emphasized as a consideration for threat during any operations across the spectrum of conflict. This trend certainly helped to raise the visibility of terrorism and terrorism-related programs, literature, and funding among the constituent services. Along with literature on weapons of mass destruction, which is considered a tactic of terrorist, terrorism has become the buzzword for installation defense planning and resourcing. It has also highlighted existing sources of literature relating to homeland defense, including *The Installation Commanders Antiterrorism Handbook*, the *Antiterrorism Force Protection Installation Planning Template;* and Training Circular 19-16 *countering Terrorism on US Army Installations.*

Among the trends in joint threat doctrine is a trend toward specificity. The advantages and disadvantages of specificity are discussed in chapter 4. This leads to the hypothesis, that while joint doctrine may have developed a more sophisticated methodology for determining threat, it may not be general enough to consider and accommodate all viable threats.

Regulations and Legal Doctrine

The most important literature category related to homeland defense or domestic security is that body of literature that governs its operations. This literature includes those laws affecting military support to civilian authorities and DoD, Army regulations,

and, in a few cases, joint and Army doctrine. With respect to homeland defense operations and domestic security, it is unfortunate that most literature does not focus so much on what the Army can do, as it does on what the Army cannot do.

Briefly mentioned in chapter 1, there has been a customary separation between military authority and civil operations which stemmed from the late eighteenth century that passed into US laws with the Posse Comitatus Act of 1878. Except for special circumstances, expressly authorized by the Constitution or an act of Congress, this act prohibits the use of the military to execute civil laws. While the Posse Comitatus Act primary purpose is to prohibit the use of the military to directly assist in civil law enforcement activities, it also prohibits other types of military operations within the civil sector and, most specifically, those against US citizens. The following *US Codes* are the source of this prohibition:

1. 18 USCA 1385: Ascribes the Posse Comitatus Act

2. 10 USCA 375: Requires the Secretary of Defense to "prescribe regulations" limiting military involvement in conjunction with civil officials (Title 10, US Code, vol. 375, 1998).

Frequently, court interpretation has supported the separation between military and civil authority. Generally, the Court has held that military support short of actual search, seizure, arrest, or similar confrontation with civilians is not a violation of the Posse Comitatus Act. Permitted support includes traffic direction and the supply of information, equipment, and facilities. Court interpretation, however, continues to evolve in appellate cases where the defense has alleged violations of the Posse Comitatus Act by military-civil law enforcement practices. Some sources suggest evidence of a new trend

with the increasing latitude for activities pursuant to military purpose doctrine. The challenge may center on the problems associated with court documentation: Courts only document "case findings" under the appellate system, which may rule out important findings with respect to either Posse Comitatus or military purpose doctrine.

All Army and DoD regulations governing either military support to civil authorities or military operations in the domestic environment implement the Posse Comitatus Act. For the purposes of this study, these regulations can be divided into to categories: those generally governing military support to civil authorities and those specifically governing military operations in the domestic environment or against US citizens. Examples of regulations from both categories are provided below.

Military Support to Civil Authorities

1. DoD Directive 5525.5, *Cooperation with Civilian Law Enforcement Officials,* 15 January 1986.

2. DoD Directive 3025.1, *Military Support to Civil Authorities,* no date.

3. DoD Directive 3025.12, *Military Assistance for Civil Disturbances,* 4 February 1994

4. DA Regulation 500-51, *Support to Civilian Law Enforcement,* 1 August 1983

Military Operations in the Domestic Environment or Against US Citizens

1. Executive Order 12333, *Procedures Governing the Activities of DoD Intelligence Components that Affect United States Persons,* December 1982

2. DoD Directives 5200.27, *Acquisition of Information Concerning Persons and Organizations Not Affiliated with the Department of Defense,* no date

3. DoD Regulation 5200.8, *Security of Military Installations*, 25 April 1991

4. Army Regulation 381-10, *US Army Intelligence Activities*, 1 August 84

Contrary to the legal restrictions of Posse Comitatus, laws, court findings, and regulations also provide some exceptions for military support to civil authorities, as well as military operations in the domestic environment. As mentioned earlier, exceptions, such as the military purpose doctrine and the inherent authority and responsibility of a commander to maintain law and order and protect the inhabitants of an assigned area of responsibility (AOR), provide some latitude for conducting military law-enforcement operations under similarly prohibitive conditions. These exceptions and associated trends are discussed in chapter 4, with some conclusions and recommendations for negotiating the complications and liabilities of these exceptions provided in chapter 5.

CHAPTER 3

RESEARCH DESIGN

This chapter provides the methodology used to evaluate how the Army's counterintelligence elements currently conduct and could legally increase operations against domestic threats in support of homeland defense. It explains the method for analyzing current literature with respect to three questions: (1) How does the Army determine the homeland threat? (2) What are the legal parameters for conducting counterintelligence in support of homeland defense? And (3) how do the first two questions affect current processes for conducting counterintelligence in support of homeland defense? This chapter also describes how current DoD, joint, and Army doctrine, regulations, policy, and guidance will be used to establish a foundation for some proposed answers to the questions (in the form of chapter 4) and chapter 5 conclusions. Finally it demonstrates how the latest experience and work from Army intelligence and USACIDC in this area can be applied to improve or, at least, refine the Army's support to the homeland defense process.

Description of the Study

This study addresses how the Army's counterintelligence elements conduct and could legally increase operations against domestic threats in support of homeland defense. The current position of joint and Army doctrine are addressed with an evaluation of strengths and weaknesses. Using this evaluation as the foundation, it discusses the latest developments in conducting counterintelligence in support of homeland defense operations from an unclassified military perspective. Finally, it will

review models used by USACIDC to see if they are applicable to the intelligence community in support of homeland defense.

A review and analysis of how the Army views a domestic threat yielded the cornerstone for this study and the review of a model for determining domestic threats against the homeland. Identifying what constitutes a threat was key to the subsequent review and analysis of "how to" conduct intelligence in support of homeland defense operations. Research in this area focused on Army guidance published in regulations and field manuals.

The analysis moves into the joint arena to review the latest in counterthreat guidance. This review points to a much more specific picture than that of the Army. The joint picture focused almost exclusively on terrorism as a threat, which provides additional avenues for analysis and discussion. This specificity offers details for profiling threats and a much more sophisticated methodology for measuring their effects.

The next portion of the study encompasses a review and analysis of the legal implications of conducting counterintelligence in support of homeland defense. The analysis in this area, are based on the discussions in chapter 1, "Problem Background," concerning the legal parameters involved in conducting intelligence in support of homeland defense.

Research Analysis

Answering the primary and secondary questions of the research analysis will require some unorthodox procedures. The methodology will include elements from different research approaches, it will primarily rely on personal experience to analyze and

to assess current intelligence support to homeland defense. It also discusses models for determining threat and legal liabilities.

To answer the primary and secondary questions, the use of models may provide the best medium for outlining the conclusions. Models or templates can be used to demonstrate the complex nature of the criteria involved in homeland defense such as legal criteria, threat criteria, and areas of employment. Models will also assist with formulating the relationships between concepts and conclusions and ultimately, may be a more effective way to outline conclusions, discuss recommendations, and suggest future research in chapter 5.

Conclusion of the Study

This study concludes with the merging of techniques and procedures used by Army intelligence and USACIDC and proposes the standardization of models that address the most essential processes within homeland defense: determining threat and legally managing counterintelligence support to homeland defense. Collectively these models answer the primary and the first two secondary questions. The final two secondary questions are discussed as a theoretical conclusion and an area for further consideration in chapter 5.

Testing the validity and reliability of the proposed models for determining threat and the legal liability involved in homeland defense appears to well beyond the scope of this thesis. Testing the models run into time constraints. Preliminary validation relied upon the analysis of the strengths and weaknesses of current doctrine, common sense approach, and personal experience.

CHAPTER 4

RESEARCH ANALYSIS AND RESULTS

Introduction

This chapter reviews and analyzes three critical areas affecting homeland defense operations. As outlined in chapter 1, it is comprised of three sections: Determining the Treat: Defining Legal Parameters for Counterintelligence Support to Homeland Defense; and Conducting Counterintelligence Operations in Homeland Defense. The first section provides an analysis of problems confronting the Army's current view of domestic threat with regard to terminology and program redundancy. It traces progress in joint and Army antiterrorism doctrine, and from an analysis of antiterrorism TTP, provides some insight into USACIDC's latest domestic threat model, followed by some proposed changes in the form of a new threat model. The second section reviews the legal implications affecting counterintelligence processes, and the latest guidance and from this analysis presents and discusses a new model for legally managing intelligence in support of homeland defense operations. Finally, the last section discusses the implications of the first two sections on homeland defense operations. It integrates conclusions from the previous sections to offer some answers to the primary question, "How should the Army's counterintelligence elements legally increase operations against domestic threats in support of homeland defense?"

Section I: An Analysis of Domestic Threat Doctrine

Homeland Defense must be tied to an accepted, common understanding of the all threat categories. Without this understanding, development of subsequent doctrine will

continue to be diffused among different programs, operations, and services. Conceptual standardization is also important because it is this shared understanding of threat that provides the foundation for managing homeland defense. At its most basic level, it should explain what constitutes a threat, and at most complicated levels it should provide threat classifications, methodology for determining threat priorities, and procedures for threat elimination. Any success at more complicated levels, begins with success at the lowest level: formulation of an agreement on a common understanding of what constitutes domestic threat.

Discussed in this section are the disputes concerning the development of current domestic threat doctrine. It starts by stressing the importance of the link between defining domestic threats and conducting homeland defense. It explores some of the unanswered challenges in establishing this link because of the mix up created by a lack of information in a comparably underdeveloped field, and by too many vague variations in terminology and definitions. Identification of a common threat doctrine has also been confounded by inconsistencies in defining domestic threat across other emerging areas including programs such antiterrorism, force protection, and security, and operations such as domestic, peace, and humanitarian.

An analysis of the challenges affecting homeland defense operations would not be complete without some discussion concerning the military's current focus on terrorism. Terrorism is considered the most probable threat in the domestic environment, while still presenting a formidable threat in the full range of "stability operation and support operation" scenarios (FM 3-0 2001, 8-1). Combating terrorism has fostered interagency, inter-service, and international collaboration, enabled resources, and provided insight in

determining, measuring. and countering such activities. This early incentive offers more than its intended value; antiterrorism doctrine offers insight and ideas beyond countering a single threat that may be applied to a broader range of threats. On the other hand, improvements in antiterrorism doctrine have been at the expense of countering other potentially viable threats in the domestic environment. Antiterrorism took the largest share of funding, resourcing, and publications. These implications of a threat policy leaning toward terrorism are further developed in subsequent paragraphs, and reconciliation between its successes and shortcomings offered in the form of a new model.

Linking the Threat and Homeland Defense

The understanding of potential threats such as terrorists, drug traffickers, and extremist is key to conducting homeland defense operations. A clear picture of the threats' intent, capabilities, history, etc. is requisite to planning countermeasures to deter, detect, detain, or defeat them. The Army's opposing forces doctrine provides a good example of a well-developed linkage between the threat (in this case, the enemy) and the intelligence processes essential to countering the threat. The linkage allows planners to project themselves into the enemy's decision cycle to plan, predict, and prepare for counteractions. A clear understanding of the enemy's, history, intent, and capabilities, allows planners to use the military decision-making process (MDMP) to develop both the enemies' "most likely" and "most dangerous" courses of action. This also allows the development of plans and contingencies to counter enemy actions. Also, the MDMP process allows planners to focus intelligence assets to confirm or deny enemy actions and either execute the plan, initiate a contingency, or reinitiate the planning process.

Defining what constitutes a threat, then, is The first step in homeland defense should be to determine what constitutes a threat. This will assist force protection and security managers, law enforcement, and intelligence agencies to focus their collection efforts. As mentioned in chapter 1, identifying the threat allows commanders to appropriately plan defenses, allocate resources, and tailor counter-threat responses. This identification process should occur at two levels. The first level should be established in doctrine, SOP or as a part of designated threat TTP. This level represents the body of knowledge concerning domestic threat. It should encompass the types of threat groups, their activities, and their potential effect on targets in the domestic environment.

The second level occurs at installation level as part of installation security and force protection activities. It started when commanders and staffs first developed the local threat scenario based on solid doctrinal concepts of domestic threat, and then tailored it to the particular aspects associated with their security environment. This second-level refinement is shaped by homeland defense procedures and takes into account the target values and other local variables.

Analysis of Current Threat Doctrine

In peacetime, defining the potential threat in the domestic environment has not been easy, and efforts over the last decade to establish standard criteria have met with only limited success. Publications designed to develop, expand, or clarify a realistic threat have been marked as much by distractions associated with their own proliferation, as they have by any progress toward integration and standardization. Guidance published in military regulations and field manuals (FMs) throughout the 1990s were plagued by an effect, where continuous development had outrun the blueprint design.

Threat doctrine is puzzling. Scanning any number of regulations or FMs concerning the definition of threat or any topic related to threat will provide numerous examples of "program cannibalization," where threat programs or concepts literally try to consume each other. They often include other programs, concepts, or common elements or even provide many of the same functions or measures to counter a threat. A quick review of some common definitions displays this pattern of similarity:

> Force Protection: Security program designed to protect soldiers, civilian employees, and family members. Facilities, and equipment, in all locations and situation, accomplished through planned integrated application of combating terrorism, physical security, operations security, personal protective services, and supported by intelligence, counterintelligence, and other security programs. . . . The four components of force protection are: operational security and deception operations; the soldier's health and morale; safety; and the avoidance of fratricide. (FM 101-5-1 1997, 1-69)

The definition of force protection from JP 1-02 does not include the four components. Although force protection includes the four components in FM 100-19, it also integrates *law enforcement operations,* and JP 3-07.2 omits "the four components of force protection."

> Security: (JP1-02) 1. Measures taken by a military unit, an activity or installation to protect itself against acts designed to, or that may, impair its effectiveness. 2. A condition that results from the establishment and maintenance of protective measures that ensure a state of inviolability from hostile acts or influences. 3. With respect to classified matter, it is the condition that prevents unauthorized persons from having access to official information that is safeguarded in the interests of national security. (NATO)--a condition that results from the establishment of measures which protect designated information, material, personnel, systems, components, and equipment against hostile persons, acts, or influences. (FM101-5-1 1997, 1-138)

> FM 100-23 provides a more specific threat to security operations.

> Security: In peace operations, security deals with force protection as a dynamic of combat power against virtually any person, element, or hostile group. These

> could include terrorist, a group opposed to the operation, criminals, and even looters. (FM 100-23 1994, 16)
>
> Protection: Operational protection also includes . . . employing operations security (OPSEC)--to include physical and personnel security, and conducting deception. (FM 100-8 1997, 3-0)

The similarity of these definitions provides some points of redundancy: (1) most of them afford similar counterthreat guidance or services; (2) although disguised by different terminology most of them are comprised of the same components or elements; and (3) most of them counter the same general threats. Terminology, such as protection, force protection, operational protection, antiterrorism, and security, all provide similar guidance for countering threats. A comparison of those definitions outlined above indicates that these definitions vary only slightly from one to another. Essentially, when installations, organizations, or persons are conducting security or force protection operations, protecting the force, practicing protection, or homeland defense, they are doing the same thing.

Programs or concepts containing many of the same elements or components create the second point of redundancy. These include operations security, deception operations, physical security, combating terrorism, safety, personal protective services, and soldier health and morale. Force protection, security, and protection are core terms that contain a component of personal security or personal protection and asset loss prevention. These elements or components are subordinate to larger catchall programs, and may also serve as major stand-alone programs in their own right, governed by their own respective regulations or literature and included as a separate and independent subject in a variety of FMs or regulations. Safety afforded an example of both: although

it is a component of force protection, it is also covered by its own regulations, and is included as a separate topic in FM 100-23, *Peace Operations* (FM 100-23 1997, 37).

Additionally, program components or elements may include each other as part of their definition. For example, combating terrorism and physical security are both integrated as part of force protection: antiterrorism is included as an appendix to the Army Physical Security Regulation AR 190-13. In reverse, JP 3-08.2, *Joint Tactics, Techniques, and Procedures for Antiterrorism*, includes physical security measures and the physical security related measures of building and lock security in several of its appendices (JP3-07.2 1998, D-1). Force Protection's latest definition, states that it is a "security program designed to protect . . . through planned and integrated application of combating terrorism, physical security, operations security, personal protective services, and supported intelligence . . . other security programs"(FM 101-5-1 1997, 1-69). What other "security programs" is it referring?

The final point of redundancy results from the fact that much of the Army's terminology provides guidance against a general, rather than a more specific threat. The threat picture is very general, any concept or program countering it seems to be overlapped by others. Except antiterrorism, any one of the aforementioned counterthreat concepts and programs provided guidance against a broad array of threats, most everything from terrorism to a group opposed to the operation to criminals and looters. Even the new FM 3-0 skirts this problem, citing the traditional broad array of threat activities "that include terrorism, illegal drug trading, illicit arms and strategic material trafficking, international organized crime, privacy, and deliberate environmental damage" (FM 3-02001, 1-8). Additionally, "extremism, ethnic disputes, religious rivalries, and

human disasters contribute" to the threat problem (FM 3-0, 2001, 1-8). In the final analysis, such general threat descriptions are not much more insightful than the catchall definition for security provided in *Operational Terms and Graphics,* which describes things that must be protected against "any hostile acts, persons, or influences" (FM 101-5-1 1997, 1-138).

The advantages of such a general view of a threat are that any or all programs or concepts can easily accommodate it and threats can be addressed by any number of measures provided by any number of programs and resources.

The disadvantage is that such a general view fails to develop a realistic or probable threat picture. Without a central focus, it diffuses counterthreat guidance and activities across a wide variety of concepts that create layers of redundant programs, systems, and measures; with little regard for force or resource improved integration and coordination, they present an overwhelming and complex set of requirements.

The cumulative effects of such redundancy may have created competing programs that duplicate requirements, confuse counterthreat responsibilities, and or compete for the same resources. As a result, some intelligence and security representatives often spend more time and energy coping with program requirements rather than countering the local threats. Instead, threat management must continue to sort through a litany of concepts and programs to develop counterthreat measures defined as much by the number and types of program, as by any indication of threat.

Focusing on the Terrorist Threat

Prior to 1990, doctrine seemed to focus on a much broader array of dangers confronting personnel, including the effects of weather, human exhaustion, and

operational negligence. In addition to antiterrorism, force protection programs focused on law enforcement, safety, physical security, and information security. Over the last decade, the trend shifted to focusing on terrorism as the largest threat to force protection and domestic security.

During this evolutionary period, force protection doctrine became increasingly associated with antiterrorism. As antiterrorism is an element of force protection, titles of force protection manuals and other literature often included both "force protection" and "antiterrorism," creating the common abbreviation "FP/AT." This placed the emphasis on terrorism as a threat on equal par with all other threats combined. And if perception is reality, future senior leaders attending the US Army Command and General Staff College confirm this emphasis. An informal survey of fifty colleagues at the US Army Command and General Staff College (class 2001-2002), found that forty-eight answered "terrorist or terrorism" to the question, "What is the number one threat within US boundaries?" With regard to the other two respondents, one answered "asymmetric threats" and the other "bombing." Of the latter two respondents, the first describes a larger threat category that includes terrorist, and the second describes a common terrorist tactic (JP3-07.2 1998, 11-2).

Determining whether or not antiterrorism is a subordinate element of force protection is irrelevant to this study. Today's antiterrorism policy continues to dominate domestic defense planning and execution, supported by a strong field of recent antiterrorism publications and literature, including the *Joint Tactics, Techniques, and Procedures for Antiterrorism;* the *Antiterrorism Reference Library;* and the *Installation*

Commanders' Antiterrorism Handbook. And most publications covering other forms of security protection usually include more than just a casual reference to terrorism.

New emphasis on terrorism has its advantages. As discussed earlier, the area concentrating on terrorism provided some notable exceptions to threat redundancy. It offers a program that is focused on a single threat group "terrorists." Inspired by domestic attacks at the Pentagon, New York, and Oklahoma, combating terrorism has become a vibrant program, consuming a share of attention, money, and resources. For a majority of the last decade antiterrorism initiatives and measures have competed in the areas of security and budgeting for additional resources, such as "victory over terrorism" (commonly referred to as VTER) funding. As joint doctrine has turned its attention to focus more and more on asymmetric threats, antiterrorism has become the centerpiece of its doctrine.

This emphasis on terrorism has provided some important benefits to the field of domestic security. It has heightened US awareness of the dangers of asymmetric threats to the American homeland. It has forced Congress to rethink current laws with respect to the balance between individual freedoms and domestic security. According to the *Navy Times,* the Senate passes yet another amendment to the Posse Comitatus Act in 1995 that would "allow the US Attorney General to call in the military when terrorists have used or threaten to use chemical or biological weapons. Since 1982, the law has allowed the military to be called in on cases involving nuclear weapons" (Maze, 1995, 9). Such changes, with regard to the use of the military in support of civil law enforcement, confirm the general willingness to reevaluate traditional values outlined in the constitutional and legal systems, as well as a trend toward reevaluating the role of the

military for countering domestic threats. Also, the focus on terrorism has generated three other essential benefits: (1) it has focused the tactics techniques and procedures (TTPs) aspect of threat doctrine, (2) it has marshaled resources for all programs willing to provide antiterrorism measures, and (3) it generated the drafting of additional publications.

Expanding Joint Antiterrorism for a New Threat Model

Combating terrorism may still have some room for improvement. A review of the definition for terrorism from JP 3-07.2 provides the basis for the subsequent analysis:

> The calculated use of unlawful violence or threat of unlawful violence to inculcate fear; intended to coerce or to intimidate governments of societies in the pursuit of goals that are generally political, religious, or ideological. (This term and its definition replaces the existing term and its definition and is approved for inclusion in the next edition of JP 1-02.) (JP 3-07.2 1998, GL-5)

The definition of terrorism has several key elements essential to understanding terrorism as a threat. First, the definition does not actually describe what the activity is, but rather describes its intent and purpose. Disputably, all domestic threat activities are unlawful. So it is the intent that is decidedly different from that presented by other threats. The intent of terrorism is to create fear and chaos. Its purpose is to coerce or intimidate governments or authorities in the pursuit of goals that are generally political, religious, or ideological.

From this definition of terrorism, emerges the dangers of an "extreme" type of threat, but "is it only the criminal group or type posing a threat against the domestic Army?" Joint Pub 3-07.2 offers an answer to this question in its own introduction:

> All acts of violence against the US military are not necessarily terrorist actions (e.g., murder or robbery). The measures contained within this publications provide guidance that will help protect the military unit and service member from

> these acts of violence as well as those committed by terrorists. (JP 3-07.2, 1998, II-11)

The passage above offers two important acknowledgements to the emphasis placed on terrorism. The first is its recognition that terrorism neither constitutes all acts of violence against the US military, nor can terrorists be considered the only threat group. The second acknowledgement is that antiterrorism measures can be applied to protect the military from nonterrorist-related acts of violence, as well as those committed by terrorists. Both acknowledgements provide important implications for determining domestic threat.

This joint publication also develops the ideas that not only are there multiple threats, but distinguishing between these types can be rather difficult:

> In peacetime military operations, there is no definitive method of differentiating terrorist acts from other violent crimes because the perpetrator's intent may be the only discriminator. A rule of thumb that can be applied is if the act is obviously related to personal gain (robbery of money or high-value items) or personal motivation (hatred, love, and revenge) it is a crime, but probably not terrorist-related. On the other hand, if the acts appear to adversely affect military operations (communications facilities, fuel storage areas) or has a high symbolic value (headquarters, particular individuals), the crime probably has terrorist implications even when no claim is forthcoming. (1998, II-11)

The importance of determining the threat is the focus, but as it relates to peacetime military operations, it tends to ignore some important implications for threat doctrine. Its failed to recognize that other acts such as violent crimes will adversely affect military operations. Almost any threat act will adversely affect military operations. Drug trafficking, theft of military equipment, gang violence, or a host of other types of threat activities will degrade readiness.

Determining the threat's intent is important for planning countermeasures, but the relevance of intent is not exclusive to countering the act. This means that just focusing on threat intent will neither prevent the act in every case, nor necessarily elevate its effects. Rather, the threat model should accommodate other possible scenarios that are a consequence of other types of threats. First, unlawful acts could lead to unintended consequences that create a terrorist type incident. Such as a bungled bank robber may take a hostage. Is this scenario handled substantially different than if the hostage-taker was a terrorist?

A nonterrorist threat groups could create the second scenario by committing terroristlike acts without the intent "to inculcate fear" (or commit unlawful acts) intended to coerce or to intimidate governments or societies in the pursuit of goals that are generally political, religious, or ideological. Such acts may be the result of nothing more that "personal motivation." Hollywood provided examples in the movies, *Enemy of the State, Die Hard, True Lies*, and *the Pandora Project.*

Another example of nonterrorists committing terroristlike acts is calling in a bomb threat or the perpetration of a terrorist hoax, such as leaving a fake package at a strategic location. Motives for these acts range from boredom to anger or apathy in the workplace to misguided pranks, but in no way constitute terrorism as previously defined. The initial intent may be harmless, but the second and third order effects can create a far more serious issue. Such as terrorist hoaxes may consume huge quantities of resources, inconvenience large populations, create social stress, or tie up emergency services. Eventually, such criminal acts could have a domino effect that might lead directly or indirectly to an unintended but similar finale as a terrorist incident, maybe even leading

to injury or death. Committing emergency services to a fake bomb threat means that services may not be available for lifesaving interdiction elsewhere.

The dynamics of a criminal group is the third scenario for consideration. A criminal group may evolve by moving up or down the scale of criminality. The intent behind the perpetrator's activities may change with the rise and fall of power. This is not an uncommon phenomenon. There are examples of gangs evolving into drug traffickers, exchanging from intent to recruit members to one of profit, or an extremist group, such as a militia shifting its intent from nonlethal government protest to acts of terrorism.

Finally, the prevalence of terrorism must be addressed and balanced against resource expenditures. The terrorist attacks on 11 September 2001 claimed the lives of over 3,000 people. Prior to these attacks, most American placed very little interest in combating terrorism. In the previous decade 176 people were killed by acts of terrorism in the US. "According to FBI statistics, only 25 terrorist incidents occurred in the Untied States between 1990 and 1997. The total death tool, however, was the result of only three terrorist incidents"(Hoffman 2000, 89). In particular, the bombing of the Federal Building in Oklahoma City accounts for all but twelve of these deaths. Surprisingly, none of the victims of any of these incidents were military.

Today, terrorism perhaps dominates the collective consciousness of most Americans while incidents remain comparatively low to those of other countries and until recently comparatively low as a viable treat in terms of other US domestic incidents causing casualties or deaths. This contradiction between fear and reality has not gone unnoticed. Bruce Hoffman touches upon this division between risks and priorities in his article, "Terrorism by Weapons of Mass Destruction: A Reassessment of the Treat."

While he is certainly not advocating complacency in the face of such potential danger, he writes:

> Terrorism poses, and will likely continue to pose, a serious threat to Americans and America interests both in this country and overseas. Nonetheless, it is equally clear that there has been a tendency to exaggerate the dimensions of the treat and the strategic impact that terrorist violence has actually wrought. And by overeating and falling prey to a sense of acute fear and intimidation, we inflate the terrorists' power in ways that are both counterproductive and often divorced from reality. (2000, 89-90)

It is important to understand the implications of such oversights on homeland defense. If counterintelligence and law enforcement are to effectively counter threats, they must accept a model that consists of multiple threats. There are several apparent advantages of a model that considers the range across the entire treat spectrum. First, it would accommodate the activities conducted by the first-line defense, law enforcement organizations. Second, counterintelligence would extend its focus to include all viable threats. Third, it would recognize the connectivity between crimes; often information collected on one crime leads to the discovery of others, some of which, present a far more dangerous threat to homeland defense. Fourth, it would allow law enforcement to use known intelligence on an organization that may have changed its intent from a lesser to a more serious threat. Finally, it would place terrorism at the top, among a natural order of criminal or threat groups. After all, as recognized by joint doctrine, "terrorist acts are criminal acts" and "in peacetime, terrorist acts are normally punishable only under domestic (local) law" (JP3-07.2 1998, 111-4).

Terrorists represent one of a number of viable threats to homeland defense. Terrorism represents that "most dangerous scenario," but not necessarily the "most likely scenarios." The phrase "most dangerous scenario" is substituted for the MDMP term

"most dangerous course of action," to distinguish a threat-action by multiple groups rather than multiple threat-actions by a single group. This view of threat considers the effects of threat on a government interest from a full spectrum of possible threats. Although such a view receives little publicity, it is widely practiced among law enforcement agencies daily. This method represents the prioritization of crime in the same way that joint doctrine prioritizes terrorist threats. In fact, USACIDC did just that, as published in their Operations Memorandum 200-02. USACIDC divided installation threats into seven groups (as mentioned in chapter 1) ranging from *terrorism* at the high end, which represents the "most dangerous" but least dominant threat, to *unsophisticated crimes* at the low end, which represent the least dangerous but most dominant threat.

As shown in figure 4, the concept of multiple threat groups is provided in a new threat model. The model presents a compromise between joint doctrinal processes for conducting threat assessments and USACIDC's latest view of criminal threat categories. The model provides an improved process in which criminal categories are considered along a threat spectrum from least to most serious, and as defined by USACIDC includes: unsophisticated criminals, drug criminals, gangs or hate groups, extremists, organized criminals, saboteurs, and terrorists, respectively (Jackson 2001, 64). At each level, criminal activity can be evaluated using a modification of the joint terrorism threat analysis, in which each threat group is analyzed using six factors: existence, capability, intentions, history, targeting, and security environment (JP 3-07.2 1998, V-7).

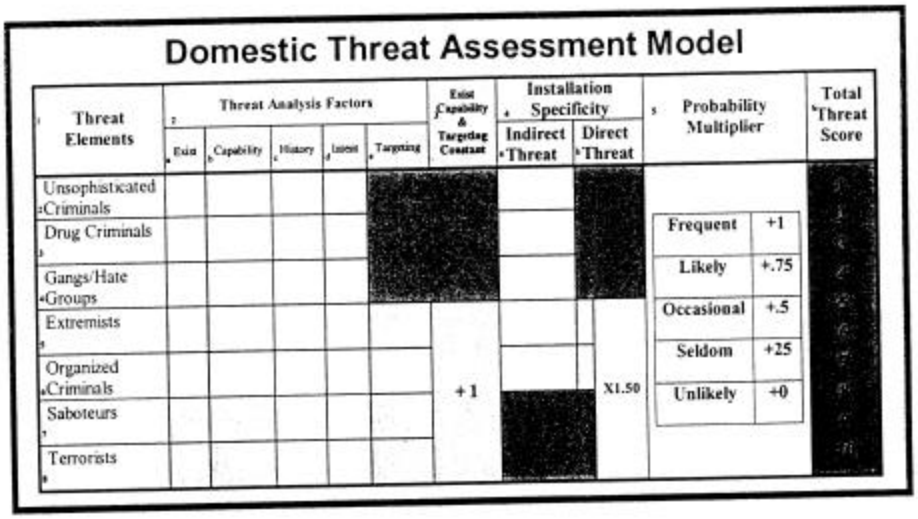

Figure 4. Domestic Threat Assessment Model for Army Installations. Source: USACIDC 2000, 3.

In addition to arranging the threat groups in column 1 from least to most serious, the model also includes additional weightings in columns 3 and 4. These methods of weightings provide a distinction between the potential adverse effects of different threat groups and are marked by shading out certain boxes to prevent entering a checkmark (for example rows 2, 3, and 4 for columns 2e, 3, and 4b; and rows 7 and 8 for columns 4a). This is a result of the four most serious threat groups (extremists, organized criminals, saboteurs, and terrorists) would generally include the combined threat factors of *existence, capability,* and *targeting.* These, are the only factors that can receive the *exist, capability, and targeting constant for an additional point* and the multiplier of *1.5* for demonstrating a direct threat to the installation. Also, saboteurs and terrorists, the two most serious threat groups, by their very nature represent a direct threat to an installation

and can only receive a check mark in the box annotating a direct threat, meaning that their score is automatically multiplied by 1.5. Similarly, the first three threat groups (unsophisticated criminals, drug traffickers, and gangs and hate groups) can not, by definition, target an installation and, therefore, cannot receive a point for targeting. The same is true concerning the point for the *exist, capability, and targeting constant,* and the direct threat multiplier of 1.5. To the contrary, a threat group receives a point for each block that is checked in columns 1 through 4, and the appropriate points added from column 5. Accordingly, the last four threat groups are the only groups that can receive a total threat score between one and ten points, while the three least serious threats can only receive a score between one and six points (USACIDC 2000, 2).

Total threat scores recognize and provide an important contrast between the frequency, pervasiveness, and effects of threat groups. This contrast goes back to the previous discussion about the most dangerous versus the most likely threat scenarios against an Army installation. The first three threat groups can affect an installation through the frequency and pervasiveness of their crimes; their effects and the installation are limited by their capability and intent. That is not to say that they cannot adversely affect an installation. They can recruit members from the Army or any other service population, commit crimes for money, and in extreme cases, even target certain persons. If their intent changed for some reason to include more serious effects, then they have probably formed into a more serious threat group, such as organized criminals or an extremist group.

The four most serious threat groups, in particular the two most serious, can receive a score from 1 to 10. Considering the fact that they can receive a low score

attests to the fact that they probably will not represent the most likely threat scenario. A possible score of 10, however, provides consideration for their potential effects in the most dangerous threat scenarios. Limiting the score of 7-10 to the four most dangerous threat groups also takes into account the target perspective. It accounts for the security environment associated with most CONUS Army installations.

Section II. Defining Legal Parameters for Conducting Counterintelligence for Homeland Defense

In addition to a continuous evaluation of threat, the Army faces the rigorous challenge of developing methodology on how to legally manage counterintelligence operations in support of homeland defense. As discussed in chapters 1 and 2, there are numerous sources that provide information concerning the limitations and liabilities associated with conducting intelligence operations in the domestic environment. This trend presents the Army with a Catch 22 dilemma: on one hand, counterintelligence elements are expected to proactively counter threats in their areas of interest before threats can adversely affect assigned interest, but on the other hand, counterintelligence elements must avoid the risk associated with civil-military violations that could result from such aggressive tactics.

Factors Limiting Army Counterintelligence in Homeland Defense

Contrary to the competing interests that stem from increased institutional pressure to conduct predictable intelligence against domestic threats on one hand, and regulatory guidance and traditions that caution Army officials from such activities on the other, very little guidance in support of either side has surfaced to resolve the dilemmas. Prior to the attacks on 11 September 2001, based on the historically low incidence of serious threats

to domestic interest, the trade-off between risks and rewards seems underbalanced. With only foresight to be gained if a serious threat strike should occur and balanced against the potential risks associated with Posse Comitatus violations, few commanders were willing to conduct aggressive counterintelligence operations in such a low-incident-rate environment. Currently, many agencies are willing to develop proactive counterintelligence programs and must contend with numerous barriers associated with civil-military law enforcement, including: (1) the complicated nature of regulatory and legal guidance in this areas, (2) potentially harsh legal penalties for violations of the Posse Comitatus Act ($10,000 or two years confinement), (3) potential professional and personal susceptibly resulting from such violations, and (4) the difficulty of implementing change in an Army culture based on customs and continuity.

Of the barrier to conducting counterintelligence in support of homeland defense operations, it is the lack of regulatory and legal guidance that presents the most difficult obstacle. There is little civil-military law enforcement guidance in general, but even less guidance related to the smaller military/army counterintelligence place of homeland defense. Even in those sources that include reference to counterintelligence, it is only briefly mentioned it in passing. For example, FM 100-19, *Domestic Support Operations*, limits its discussion of intelligence operations in reference to law enforcement activities to only a single page. It begins with this general introduction with references to military intelligence personnel, but could very well be applicable to military police:

> Use of MI personnel during domestic support operations in restricted as a direct result of lessons learned from their improper use in the 1960s [during protest demonstrations]. Consequently, LEA [law enforcement agency] requests for MI personnel or material for counter-drug support must be approved by the Secretary

> of the Army General Counsel and coordinated through the Department of the Army Office of the Deputy Chief of Staff for Intelligence. (FM 100-19 1993, 3-5)

The FM also describes some of the authorized intelligence activities that are allowed under disaster assistance operations; these operations are currently included under the category of *support operations* in FM 3-0. This guidance can probably be applied to other parallel operations that are characterized by a clearly defined military connection. By chance, this is similar to the guidance published by USACIDC and discussed later in this chapter.

> However, a specific MI mission statement, coordinated through proper authorities, must authorize MI personnel to collect, analyze, and disseminate information. When so authorized, MI personnel may--
>
> 1. Acquire information that may threaten physical security of DoD employees, installations, operations, or official visitors, or that may be needed to protect the safety of any person, that is, force protection.
>
> 2. Analyze and disseminate information to disaster relief personnel and emergency operations centers (EOCs).
>
> 3. Support EOC operations using "intelligence preparation-of-the-battlefield (IPB)" skills. (FM 100-19 1993, 3-5)

Regulatory guidance seems even less understandable. The same point is discussed in USACIDC's Operations Memorandum 002-00 as an introduction to its legal appendix, which provided initial legal guidance to USACIDC personnel for conducting DTIM operations. This memorandum points out, that the regulations are "complicated and unclear," and that their mandate does not apply to authorized law enforcement activities. USACIDC's legal guidance published in 2000 is introduced in the following passage:

> The collection, processing, storing and disseminating of information concerning persons and organizations not affiliated with the Department of Defense is

> governed by DoD Directive 5200.27. This Directive was issued in 1980 and is currently undergoing a rewrite. It provisions are both complicated and unclear. Unfortunately, the Army regulation which purports to implement DODD 5200.27 is dated 1974, has never been updated by its own terms does not apply to authorized criminal investigation and law enforcement information gathering activities. (USACIDC, 2000, B-1)

The Legal Problem with Decentralization

In the absence of centralized guidance and little regulatory precedence, the Army tends to segregate interpretation and decisions for civil-military guidance by delegating such activities to local installations. Accordingly, legal guidance for conducting DTIM is also delegated to local levels to be deciphered installation by installation. The adverse aspect to this avenue is that authority and legal experts at higher levels are usually uninformed, or often remain silent, and guidance, if provided, is usually general and on an issue-as-needed basis. This means that DTIM operations can waver dangerously in one of two ways: they can either become mired down by local systems and processes, become reactive rather than proactive, and unavoidably, become unresponsive to real-time processing; or operate in isolation without due legal prudent and often unrelated to formal threat-focused guidance from the installation commander or other force protection participants. In most cases the DTIM process is given far less attention than that posed in either scenario but, instead, remains on the confines of security and law enforcement interests.

Decentralizing DTIM creates other requirements related to system inoperability between counterintelligence and law enforcement organizations and agencies. The Provincial nature of DTIM often leads to an inability to communicate between installation, between lower and higher organizations, and between internal and external

agencies. The use of different terminology or intelligence processes means that agencies can experience problems while working together. The difference in terminology can affect legal guidance and create fundamental differences in law enforcement procedures. Techniques and procedures permissible to one agency can be considered legally intrusive to another.

Disagreements in DTIM terminology, procedures, or legal guidance may also create confusion or duplications of efforts among agency responsibilities and authority during joint investigations, and during other collaborative processes, as well as slanting incident reporting standards. A lack of legal guidance or opposing legal guidance may complicate procedures or jeopardize the adjudication process, such as invoking the exclusionary rule or even lead to the dismissal of a case. The lack of confidence from underdeveloped guidance or procedures may also restrict intelligence dissemination. Figure 5, Counterintelligence Reports, Addressees, and Formats, displays a partial list of agencies where Army counterintelligence reports are disseminated. Because of the legal liabilities associated with DTIM, many organizations are reluctant to cooperate or share information concerning intelligence and law enforcement activities. Finally, the decentralization of DTIM may lead to different reporting standards. An incident viewed and reported as a serious threat by one agency may only be viewed and reported as a modest or negligible threat by another agency.

(U) Addressees and Formats

5–7. 6-8. INFORMATION REPORTED	ADDRESSEES	APPROPRIATE REPORT
Theater-level Requirements	J/G-2 and affected commands	Intelligence Information Report
Critical information to the commander, if directly related to force-protection	Commander of affected units, theater Force Protection elements, and organizations specified in AR 525-13, if applicable	Spot Report
National-level Requirements	Defense Intelligence Agency; J2CI; Army Counterintelligence Center; Army Collection Manager	Intelligence Information Report
Terrorism-related information	Anti-Terrorism Operations and Intelligence Cell, DIA, ACIC, applicable theater Force Protection elements, INSCOM and organization specified in AR 525-13, if applicable	Intelligence Information Report
Counterintelligence investigation (closed)	Upon case closure send to DIA, ACIC, and INSCOM	Intelligence Information Report
Counterintelligence Investigation (open)	**Coordinate with the Army CI Coordinating Authority prior to publication.** Once approved by the Army CI Coordinating Authority send to DIA and ACIC	Intelligence Information Report
Foreign intelligence and Security Service information derived from Offensive Counterintelligence Operations	When possible, sanitize information and publish an IIR to DIA, ACIC, and INSCOM. In cases where information cannot be sanitized to protect the operations, provide hardcopy information to ACIC, INSCOM, J2CI, and other organizations conducting OFCO	Intelligence Information Report
Counterdrug information	The appropriate Law Enforcement Agency. When responsive to a validated collection requirement, publish an IIR and send to DIA, ACIC, and INSCOM	Intelligence Information Report
Information concerning protected personnel of the US Secret Service	Route immediately to the US Secret Service	Use fastest method. Telephonically, then Electronic Message or Summary of Information (SOI) memorandum

Figure 5. Counterintelligence Reports, Addressees, and Formats. Source AR 381-10 1999, 5-7

Analyzing Legal Findings of the Appellate Courts

A review of legal complications from the law enforcement side may provide insight into issues that counterintelligence elements can expect when conducting operations in support of homeland defense. The legal interpretation of the law as it applies to conducting DTIM may vary based on the nature of the particular law enforcement activity. Law enforcement operations countering drug trafficking and activities countering terrorism provide examples in variations of how military services interpret the Posse Comitatus Act based on appellate court decisions. Both areas have

seen recent change. On one hand the legislature made several exceptions to the Posse Comitatus Act, while on the other, an improved understanding of the legal implications in the civil-military arena continue to emerge under the interpretations of the appellate courts. Recent legislative changes granting some exceptions to Posse Comitatus are discussed as a part of chapter 5 conclusions regarding the future of civil-military law enforcement activities and, particularly, DTIM. However, attention here is focused on the more immediate and applicable changes created by the appellate courts.

Individual services may have a different perspective of the legal permissions and exclusions involved in conducting counterintelligence and law enforcement based on appellate court records and holdings in their own respective criminal cases. Unluckly, research in this area is limited primarily because only the appellate courts provide case documentation. Regardless, the implications of discovery in this area are enormous and well worth the search. Each court holding adds to the growing body of knowledge concerning civil-military law enforcement. Also, any precedent that is established provides more information regarding the legal permissions for conducting DTIM and clarifying the Army's counterintelligence role in homeland defense. By examining some of the important cases along this line of inquiry, the Army will be able to refine its guidance for conducting DTIM to create a better balance between the rewards of proactive threat countermeasures with the risk associated with operating in the domestic environment. Even though a comprehensive analysis of current legal interpretation is beyond the scope of this research, the following examples from appellate decisions provide an appreciation for the differences, complications, and insight of interpretations from the appellate courts:

> Purpose of 18 USCS, 1385 is to preclude direct active use of federal troops in aid for execution of civil laws; passive activities of military authorities, which incidentally aid civilian law enforcement, however, are not precluded. (*State v. Nelson* 1979, 298 NC 573)

> Activities which would constitute a passive role which might indirectly aid law enforcement are mere presence of military personnel under orders to report on necessity for military intervention, preparation of contingency plans to be used if military intervention is ordered, advise of recommendations given to civil law enforcement officers by military personnel on tactics or logistics, presence of military personnel to delivery military material, equipment or supplies, to train local law enforcement officials on proper use and care of such material or equipment, and to maintain such material or equipment, and to maintain such material or equipment, aerial photographic reconnaissance flights and other like activities which would not be unlawful under 18 USC, 1385. (*US v. Red Feather* 1975, 392 F Supp 916, DC 3D)

The first two court decisions provided a foundation for the use military purpose doctrine to establish the "military connection" between the military interests and law enforcement to other civil support activities. Law enforcement activities both on and off the installation must have a purpose that is directly tied to military interests. Direct assistance to civilian law enforcement is not permissible. Any assistance rendered as the result of a passive activity or as an unintended consequence of the military purpose is permitted, but when called upon by the appropriate authority, the military can assist civil law enforcement by providing information, loaning and training personnel on the use of equipment and other materials, provide aerial reconnaissance, and prepare and train on contingency plans.

> Defense contractor's challenges to search warrant used to search plant for evidence of conspiracy to defraud government results in neither suppression of evidence nor dismissal of indictment . . . where Air Force's execution of search by its Office of Special Investigations (OSI) because actions of OSI agents were not regulatory, proscriptive or compulsory in nature and even if they were Inspector General Act (5 USCS appx 3) expressly authorized questioned conduct. (*US v. Stouder* 1989, 724 F Supp 951, MD GA)

> Participation by military personnel in drug investigation for purpose of assisting state and local agencies in investigation of cocaine distribution did not constitute posse where military participation did not pervade activities of civilian officials and did not subject citizenry to regulatory exercise of military power. (*US v. Bacon* 1988, 851, 52d 1312, CA 11 G)
>
> There was no willful use of Air Force as posse to execute civilian laws, where, consequent to off-base sting operation, in which airman was arrested during purchase of marijuana, undercover agents searched his civilian wife, took her to air force base, and detained her there, since there was independent military purpose to agents' conduct, and since Posse Comitatus Act is not intended to limit military in prevention of illicit drug transactions by active duty military personnel, whether such conduct occurs on or off military installation. (*Riley v. Newton* 1996, 94 F3d 632, 10FLW Fed C 349 CA 11 GA)
>
> Collaboration of Marine Corps law enforcement personnel and agents of federal state and local agencies does not indicate motivation of military personnel to aid in execution of federal law, but rather facts support purpose to control drug distribution involving military personnel; thru, use of military personnel does not constitute Posse Comitatus. (*US v. Brown* 1980, 9 NJ 666)

All four cases implied that it was lawful for the military to conduct investigations for a military purpose when the activities do not pervade civil law enforcement and when participation in such law enforcement does not subject civilians outside of military jurisdiction to military authority. The first case went a step further and specifically held that military law enforcement was not in violation and its actions were not "regulatory, proscriptive, or compulsory in nature."

In cases where the military is conducting an investigation with the purpose of preventing, stopping, or limiting illegal acts that adversely affect military interests civilians can be detained. Explicitly cited are incidents where the military was assisting civil law enforcement to protect to military members and control drug distribution, whether or not the investigation is conducted on or off the installation was irrelevant.

> Assistance given state police by United States airmen in investigation of narcotics cases was not in violation . . . since assistance was not induced, required or

> ordered by Air Force officials, was of a personal nature and was unrelated to his status as military man. (*People v. Brown* 1979, 94 MI App 209, 288, NW 2d 392)
>
> National Guardsmen's participation in marijuana arrest in conjunction with Drug Enforcement Administration did not violate Posse Comitatus Act, since they were not part of Army or Air Force but sate servicemen, where they had never received orders directing them into federal service, and their command had not been taken away from stat's governor. (*US v. Hutchings* 1997, 127 F3d 1255, CA 10 Utah)

The two cases above held that the status of military members is relevant to whether or not their involvement is legal. Status can be determined by their relationship to the service during their participation in civil law enforcement activities. If participation is not caused by the military or in any way enforced by the nature of the service member's official duties, then participation is probably not in violation of Posse Comitatus. Also, National Guard members are not subject to Posse Comitatus when they are not under the provisions of Title 10 or not on annual drill status. In other words, the National Guard can support civil law enforcement unless activated with current orders for active duty.

> Navy can be given exception to assist Coast Guard in its law enforcement activity. . . . [T]here is no violation of 18 USCS, 1385 in its use of Navy destroyer in pursuit, boarding, and seizure of converting fishing vessel suspected of being used of trafficking in marijuana. (*US v. Del Prado-Montero* 1984, 740 52d 113, Puerto Rico)

Just as the status of service members is irrelevant, the status of the services themselves, while providing civil-military law enforcement, is relevant to whether or not their participation is legal. This passage establishes the Navy, much like Army, is granted certain exceptions to the Posse Comitatus Act. In this particular case, the Navy may assist the Coast Guard in conformity with law enforcement. As expected, the "Posse

Comitatus Act does not apply to United States Coast Guard," because it falls under the Department of Transportation (*Jackson v. State of Alaska* 1991, 22 CrL 2338).

> Where bulk government's proof of defendants' guilt in violating federal firearms law's prohibition against sale to minors and no-residents was product of undercover investigation carried out in large part by several Marines at request of Special Investigator of Alcohol, Tobacco and Firearms Division . . . and defendant sought, both to suppress and exclude testimonial evidence produced by Marines' investigation on ground that investigation violated Posse Comitatus, court refuse to reverse conviction. *(US v. Walden* 1974, 490 52d 372, CA4 VA)

> Investigator was entitled to qualified immunity from prosecution under Posse Comitatus Act for his inactive role while members of military drug suppression team accidentally shot arrestee during handcuffing, since investigator cannot be said to have violated established law, where "willful use" of Army to execute laws had not been defined adequately by case law. (*Riley v. Newton* 1996, 94 F3d 632, 10FLW Fed C 349 CA 11 GA)

Of interest, are those cases where the courts had an indication of a violation of the Posse Comitatus Act or other intrusion, but, nevertheless, rule conservatively in support of the government or military. Numerous cases have demonstrated that a "violation of 18 USCS, 1385 does not mean that evidence surrendered by military to civilian authorities must be excluded" (*State v. Nelson* 1979, 298 NC 573) just as a "Violation of 18 USCS, 1385 does not automatically mean that evidence obtained as result of violations should be suppressed"(*State v. Trueblood* 1980, 46 NC App 541, 265 SE2d 662). In many cases, motions to exclude or suppress evidence were denied despite indications of unlawful civil-military operations. The last two cases reinforce the seemingly complicated and unpredictable nature of legal interpretation and execution in this area. In one case, the court refused to reverse the conviction even though the Marine clearly circumvented civil law enforcement operations, first at the request of civil authorities, and second, in a manner that carries out a preponderance of the work. The second case affords evidence

that even the courts are struggling with the lack of precedence from case law in areas pertaining to the Posse Comitatus Act. The conclusion that one might draw from all the appellate decisions listed above is that military members are unlikely to receive a favorable ruling when charged with violating the Posse Comitatus Act.

Establishing the Military Connection

The main points of argument in these court holdings and that of the demonstrated process of analyzing, collating, and summarizing their provisions centers on defining the military connection or relationship. Understanding court holdings and how appellate courts interpret the conduct of military law enforcement activities within the narrow exceptions of Posse Comitatus provides insights into the reasoning between what is legal and what is not. As a bottom line, the Army cannot support civil authority as its primary motive for conducting law enforcement activities unless approved by the appropriate authority. The military connection can be satisfied "as long as the military pursues the investigation of an offense (or related law enforcement activity) with a view toward establishing facts to sustain a court-martial or to pursue a legitimate military function or purpose, then any incidental investigative benefit to civilian law enforcement officials is immaterial" (Gilligan 1999,22).

Several questions still remain as the appellate court continues to interpret cases that establish precedence for civil-military law enforcement operations. Until such time as the courts have defined an adequate body of information regarding this area of the law, the Army must proceed with caution. It must take the appropriate measures to develop improved systems for both defining the military connection and training its law enforcement personnel. Meanwhile, as a body of legal precedence grows, current court

holdings may be used to improve and refine those legal stipulations already established by military regulations or other authority, such as DoD Regulation 5525.5, *DoD Cooperation with Civilian Law Enforcement Official,s* or USACIDC's Operations Memorandum 002-00. The DoD directive establishes the foundation for the military connection by providing that the following actions are among those permissible:

> 1. Investigations and other actions related to enforcement of the Uniform Code of Military Justice (UCMJ).
>
> 2. Investigations and other actions that are likely to result in administrative proceedings by the Department of Defense, regarding of whether there is a related civil or criminal processing.
>
> 3. Investigations and other actions related to the commander's inherent authority to maintain law and order on a military installation of facility.
>
> 4. Protection of classified military information or equipment.
>
> 5. Protection DoD personnel, DoD equipment, and official guests of the Department of Defense.
>
> 6. Such other actions that are taken primarily for a military or foreign affair's purpose.

Similarly, in response to formalizing DTIM operations in early 2000, the OSJA, Headquarters, USACIDC, published some basic rules on tenets for gauging the military connection. These rules were developed to provide USACIDC staff and agents with some basic policies for determining the legal parameters of conducting DTIM operations. The policies were the product of a joint effort between the OSJA and the criminal intelligence directorate and were established by creating and analyzing a series of scenarios to develop some basic guidelines for determining the military connection. Each scenario was written considering the more complex legal "gray areas" involved in conducting DTIM operations. The legal staff analyzed each scenario to determine the

legal parameters for conducting DTIM operations for each specific case, with the intent of sorting through their conclusions for some common principles that could be generalized to other DTIM situations. The following seven bright line rules were developed, approved, and published as an appendix to Operations Memorandum 002-02:

> 1. You can always assess whether you can collect, process, store or disseminate information about DoD affiliated persons or organizations. (Establishes the premise that intelligence personnel may analyze, but at this point, leave open the question of how).
>
> 2. You may always report information to other law enforcement organizations if there is evidence of a threat to life or property or a violation of law, even if you are not authorized to collect the information involved (Establishes operations at the other end of the spectrum that regard).
>
> 3. You may collect information on non-DoD affiliated persons or organizations if you have credible information that they are involved in criminal activity on a military installation.
>
> 4. You may collect information on non-DoD affiliated persons or organizations if you have credible information they are committing drug offenses with active duty personnel off a military installation.
>
> 5. You may collect information on non-DoD affiliated persons or organizations if you have credible information they are committing criminal acts that constitute a clear threat to DoD property or a direct threat to persons on a military installation.
>
> 6. Decisions on collection, retention and dissemination are extremely facts sensitive . . . consult your USADIDC legal advisor at the beginning and whenever the facts change.
>
> 7. Do not . . .
>
> a. Collect information about how people vote, their political party affiliation, what organizations they belong to, or how they exercise their constitutional rights.
>
> b. Covertly or deceptively penetrate a civilian organization (FM 100-19, 1993, B-1)

Both sets of permissible activities provide examples of important guidance for determining the military connection, but they may lack the systematic approach, method,

or process necessary to impressively train law enforcement. This list of permissible activities teaches law enforcement persons how to think about, develop, and gauge the military connection? Do such lists even contain all of the essential variables for establishing the military connection? Acquired measures can become confusing in more complex scenarios. Could counterintelligence or CID conduct domestic threat intelligence against a dangerous criminal upon request by civil authorities? Based strictly on those activities listed as permissible, the answer is probably "no." However, if civil law enforcement requested help in locating a violent and extremely dangerous suspect creeping somewhere just off post. Would either of the lists previously discussed provide insight in determining addition variables relevant and essential to defining the military connection?

Would such prescriptive measures that provide examples of what to do, rather than how to think, allow a forum for growth and charge? In this regard, the lesson from the appellate courts is powerful. Determining the military connection is often a complex process with room for interpretation, change, and growth. A more flexible model for analyzing the wide range of "gray area" scenarios may help law enforcement determine additional variable associated with determining the military connection and, ultimately, improve the real-time detection of domestic threats. At the least, it will assist law enforcement organizations in discussing the appropriate questions concerning civil-military law enforcement. It will generate more questions and hopefully, more answers.

The model at figure 6 provides one such method that might help law enforcement personnel determine the military nexus or its absence, as well as provide a system of measurements to help gauge the liabilities associated with conducting DTIM in any

particular situation. This model provides a forum that could assist counterintelligence and law enforcement to accomplish the following five functions:

1. It provides a systematic process for determining the military connection by helping to identify and articulate legal gray areas.

2. It creates a standard design for training personnel that might improve the accuracy and consistency of performing in executing laws associated with DTIM operations. Like risk management, it also generates a document for discussing the elimination process.

3. It provides a worksheet that highlights the relationship between the military connection and the intelligence process, with respect to the subsequent DTIM activities of either disseminating or strong intelligence.

4. It provides a system of measurements to help gauge the legal liability associated with conducting DTIM for any particular situation.

5. It provides an academic model to capture change with respect to laws and the subsequent interpretation of those laws. It provides an active link between the legal and regulatory statutes and any subsequent change to those mandates.

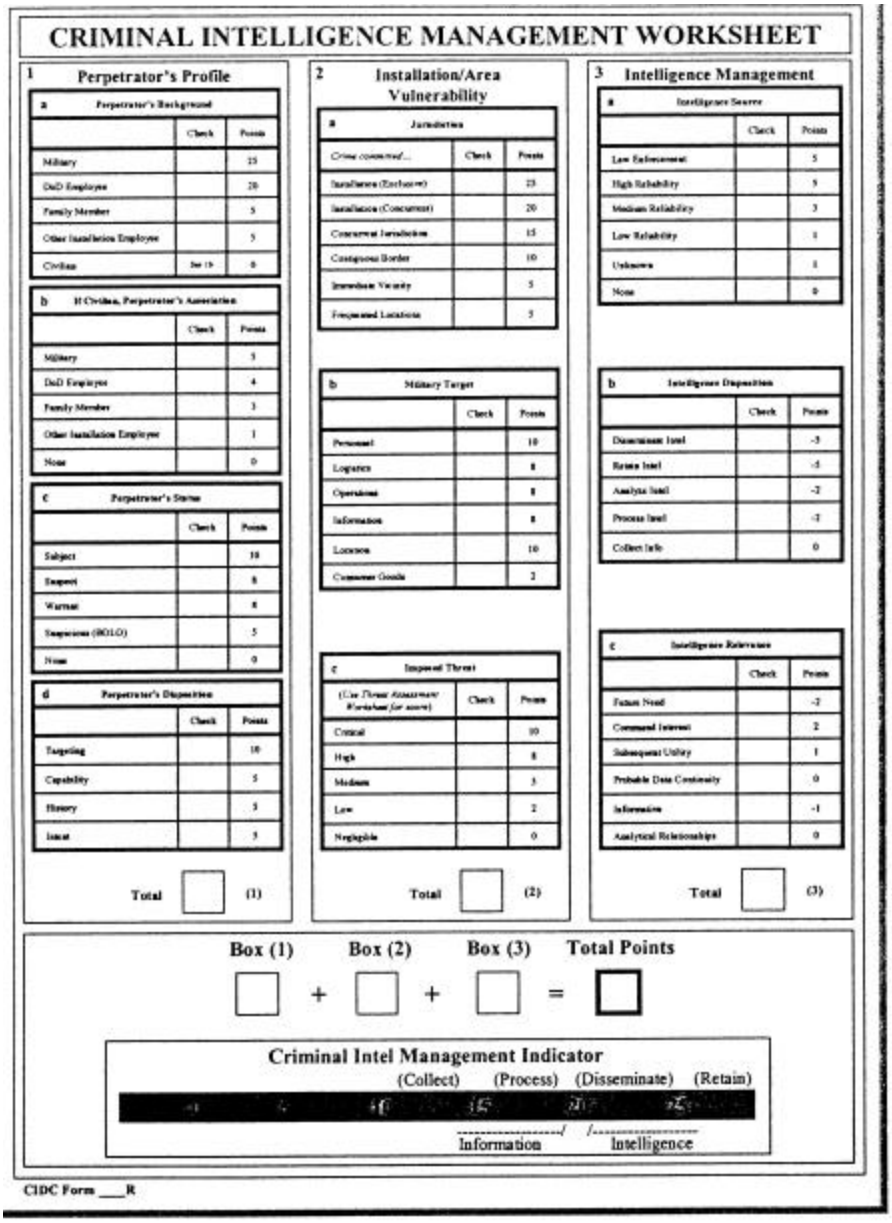

Figure 6. DTIM Assessment Model. Source: AR 195-2 1985, 3-21.

The model is comprised of three columns, labeled: *perpetrator profile, installation vulnerability*, and *intelligence management* (Jackson 2001, 81). Each column consists of several variables that represent a set of conditions that are prioritized and given a corresponding number in accordance with their respective value. Each value is used to determine the link between that particular variable and determining the military connection or risks associated with conducting DTIM. The first two columns are used to assist in determining the military connection, while the last column in sued to assist in determining the liability of conducting DTIM processes, including collecting, processing, disseminating, and retaining.

Under the *perpetrator profile* column, the variable of *perpetrator's background* is separated into five conditions, each ranked in an order based on its value of determining the military connection. A perpetrator that is military, for instance, has a higher value (25) associated with determining the military connection than does the civilian, with excluding all other variables, would offer no value for determining the military connection. Certainly this meets the legal test established in DoD Regulation 5525.5, which grants authority over a soldier under the first of those actions listed as permissible, but nowhere stipulates, excluding all other variables, authority over civilians.

With the exception of the variable of *imposed threat* in the bottom of the second column, all other variables in the first two columns are calculated and justified the same as the example of the *perpetrator's background* variable. The *imposed threat* variable receives its rating based on the threat score from the threat model presented in figure 4. Ranking and scoring of this variable are based on the principle that as the threat increases so too does the permissibility of those actions that might be considered necessary, under

the installation commander's inherent authority and responsibility, to protect the installation.

The final column (*intelligence management)* recognizes the range of liabilities associated with conducting the DTIM process. In addition to determining the military connection, this column captures what military law enforcement personnel plan to do with the information or intelligence. This is an important consideration because the activity from collecting to disseminating or retention may have a different degree of liability associated with this process. Collecting information may have relatively little liability associated with it, whereas retention of intelligence in a database may generate far more liability, especially if there is no plan or system for purging the data when it is no longer associated with a military connection. Depending on the conditions of the variables selected, points may be assessed that require a higher score in the first and second columns to offset the higher liabilities in the third column. In other words, there is a direct positive correlation between intelligence disposition and defining the military connection: the higher the liability associated with its disposition, the higher the threshold for establishing the military connection.

The points for each column are then added and annotated at the bottom. These points are then added together to come up with a total value for the DTIM worksheet. The total value can then be referenced against the criminal intelligence management indicator scale at the bottom of the worksheet. This indicator ranks liability of a scale from 1 to 25. Those ratings that fall along the "shaded" portion or below 15 probably require a stronger military connection before conducting any counterintelligence, law enforcement, or DTIM activities. Although all worksheet results should be checked with

the installation legal advisor, those rating that fall along the shaded portion or above 15 on the scale are probably indicative of all well-defined military connection. This model, must be used with caution. It is intended only as a tool to generate and improve discussion and training techniques for conducting DTIM. It results are not conclusive. As discussed in chapter 5, this model has not received extensive and independent testing. It may require improvements, such as additional variables, changes in assigned point values, or further clarification.

Section III. Integrating Figures 4 and 6 into the DTIM Process

Integrating the models at figures 4 and 6 into the DTIM process can be demonstrated both quickly and easily by using the DTIM Model from the USACIDC's Operations Memorandum 002-00. This model at figure 7 depicts the DTIM process as a cycle comprised of four phases: Intelligence Collection; Threat and Vulnerability Assessment; Crisis Management; and Analysis and Deterrence. Each phase of the model is associated with installation law enforcement and force protection requirements. These requirements include developing intelligence networks and conducting liaison activities in phase I; providing force protection services in phase II; responding and mitigating crises in phase III; and investigating, reporting, and capturing lessons learned in phase IV. Each phase is an integral part of the entire DTIM process; therefore, the requirements in one phase are related to activities in each of the other phases. Although the model demonstrates DTIM as a sequential process, it may begin at any phase and continue to the next phase or skip to any other phase. Similarly, the model demonstrates the relationship between the DTIM process and the installation THREATCONs that may

be upgraded at any point, but THREATCONs C and D would generally be associated with phases II and III, respectively.

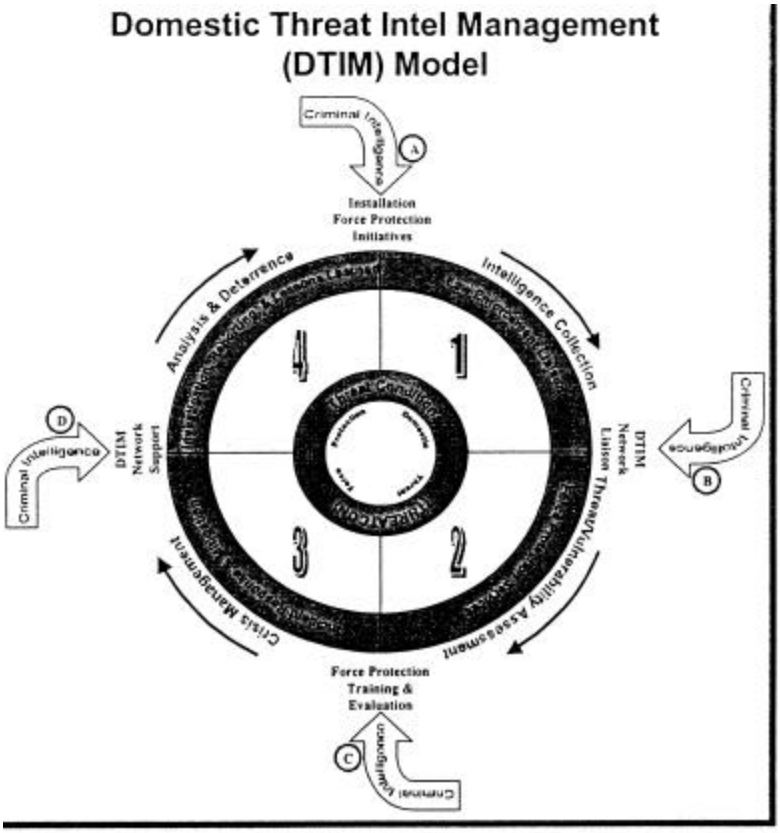

Figure 7. DTIM Model. Source: USACIDC Operations Memorandum 002-00. Source: USACID 2000, 13.

The activities associated with the threat and legal models in figures 6 and 7 generally occur during phase I activities in preparation for providing force protections services in phase II (Jackson 2001, 85). These services include law enforcement, physical security or other force protection threat, and vulnerability assessments (i.e.,

antiterrorism vulnerability, extremist criminal activities threat assessment, economic crime threat assessment, personal security vulnerability assessment, etc.).

The processes captured by these models are essential to the entire DTIM process and influence subsequent success in later phases. It is critical that the threat is well defined and priorities established through essential elements of criminal information or priorities of intelligence requirements. Likewise, the counterintelligence process must be carefully managed to ensure that violations during the domestic intelligence process in phase I do not generate subsequent or more serious violations in later phases. The worst outcome might be the dismissal of a government case against a dangerous threat group, which, consequently, would no longer lack the opportunity of a second attempt.

As a final note, DTIM processes in phase I of the DTIM Model should heed the cautions provided in appendix A of JP 3-07.2, *Joint Tactics, Techniques, and Procedures for Antiterrorism.* Its advice is borrowed from similar context and is certainly applicable to the area of homeland defense. The DTIM models discussed in sections I and II could conceivably provide

> the commander with a tool to assess the potential vulnerability of [or threat against] a base, unit, ship, or port activity, but it is [they are] not a substitute for sound judgement. These guidelines also serve to limit the scope of [DTIM] operations and are only one part of the larger issue that clearly and appropriately belongs to the traditional commanders' responsibilities for the overall well-being of service members, civilian employees, and family members as well as facilities and equipment. (JP 3-07.2 1978, A-1)

CHAPTER 5

CONCLUSIONS, RECOMMENDATIONS, AND FUTURE RESEARCH

Introduction

This chapter consists of observations concerning the results of research into the Army's counterintelligence role in homeland defense. The three major sections are Strategic Considerations, Conclusions and Recommendations, and Suggestions for Future Research. The first section considers the question of, What is next? It addresses areas that are not specifically included in other chapters, but of value and worth consideration in summary. It addresses the basic question of how the Army should legally increase its counterintelligence role in homeland defense. Current limitations imposed by Posse Comitatus and the prohibitions of collection of information on US citizens are reviewed, and insight is provided into current trends that are requiring legislators, courts, and leaders to reexamine their application when considering the use of counterintelligence in support of homeland defense. Conclusions in this section focus on the Army's strategic role in civil-military operations and more specifically, its counterintelligence role in homeland defense.

The second section offers conclusions and recommendations on the areas discussed in chapter 4. It also affords some initial guidance for counterintelligence elements. Probably the most important conclusions and recommendations involve the use of standard definitions and systematic processes for determining domestic threats and a recommendation on how the Army can legally increase counterintelligence operations in support of homeland defense. This section also discusses the need to increase visibility of legal interpretations with concerning to domestic civil-military relations,

specifically counterintelligence and law enforcement. And also explore the benefits of collaboration between agencies and their legal advisors.

Finally, the third section discusses unanswered questions and makes recommendations for future research. Without question, homeland defense is an emerging area of concern that is still relatively incomplete and fragmented. The intent of this section is to consider those areas that might provide a complete picture of homeland defense. For example, what future research might provide answers or solutions that will help consolidate and standardize homeland defense operations? Also, what areas of research might provide the necessary information to improve systems or develop processes to make homeland defense operations more effective or viable? Finally, this section discusses a need for future research to test the ideas presented in the new threat and legal parameters sections. What type of research approaches might be used to test the reliability and validity of these ideas?

Section I. Strategic Considerations

The counterintelligence process as developed and discussed in this document crosses the threshold between counterintelligence and law enforcement activities. As such, it must always be kept in its proper perspective. Counterintelligence is clearly a mission that operates in the gray area between those activities sanctioned, on one side, by executive emergency power, DoD and military doctrine, a commander's inherent authority, and those activities, on the other size, that are expressly forbidden by the Posse Comitatus Act. Consequently, counterintelligence elements supporting homeland defense must always strive to define, articulate, and follow only those activities characterized by a clear military connection.

Any conclusions and recommendations concerning the Army's counterintelligence role in homeland defense must at least consider the latest changes or trends with respect to US laws and the military regulations that implement those laws. A true appreciation for these changes can only be understood within the traditional and historical context of the Posse Comitatus Act. While this act generally prohibits use of the military for domestic assistance and particularly, for civil law enforcement, its provisions are both dynamic and complex. Its passage in 1878 did not overwrite those laws enacted to support such constitutional influences or constitutional authority. The president can and has called upon the Army under executive emergency authority numerous times in the almost 125 years to provide assistance from the enforcement of civil rights, to assist civil authorities during natural disasters, and even to provide law enforcement against national, state, and local civil demonstrations.

Recently, the traditional separation between military and civil assistance has decreased under the Army's increasing role in domestic support operations. The Army's operations tempo has increased tremendously to accommodate domestic support missions. Since 1980, the Army has participated in almost every natural disaster relief operation: supported civil law enforcement during the Los Angles riots, assisted US Customs and the US border patrol in counterdrug operations, provided assets for the consequence management process following the Oklahoma City bombing incident, and assisted in the investigation on the attacks of the Pentagon and the World Trade Center.

Participation in other operations outside the domestic threat has also sparked the imagination of civil and military leaders to the possibilities of this new role. Doctrine covering operations other than war scenarios has demonstrated the parallels between

stability and support operations at home and abroad. The doctrine covering these types of operations, both at home an abroad, treats them similarly. After the introduction of the term in FM 100-5 in 1993, doctrine covering these operations referred to them as stability and support operations and, most recently only changed slightly to stability operations and support operations in *Operations Manual* (FM 3-0 2001, 13-1).

As a result of these trends, the legislature addressed on numerous occasions the issue of whether or not to extend the authority of the military to directly assist civil authorities and, if so, to what extent. Proponents on both sides of the issue wave banners of legal doctrine and traditions and maybe a white flag from those who feel the military may be the only solution to stemming the tide of domestic threats. This debate presents the executive and legislative branches with a difficult dilemma that has emotional ties dating back even before its constitutional roots, probably originating from an eighteenth century mistrust of a large standing British Army among the early American colonies. This awareness was reinforced numerous times when the military was used to suppress local rebellions, culminating in the US Army's constabulary role during the reconstruction era in the south, just after the American Civil War.

The main point of the issue concerns the balance between providing national security and protecting the civil rights of US citizens. The question becomes: To what degree can the military be used to intrude into American lives for the sake of protecting them against domestic and transnational threats? On one side, the view of proponents for tradition was summed up during a 1995 debate on the senate floor: "Separation of military from civilian powers is rooted in our history," said Senator Larry Craig, Republican-Idaho. "We have cautiously and appropriately guarded that separation

throughout our country's existence" (Maze 1995, 9). On the opposite side, there are a series of exceptions, including the 1981 exception for assistance against drug trafficking. The 1982 exception for assistance in the event of a nuclear detonation on American soil, and the 1995 update, to provide assistance against terrorism and threats of chemical and biological use, provides a narrowly defined set of situations in which the military can be utilized.

These exceptions may or may grant substantial permission for military involvement in civil law enforcement, but they proclaim a trend in that direction. An article from 1986 in the *Bulletin of the Atomic Scientist* predicts the possibilities:

> Despite the 1878 Posse Comitatus Act which prohibits use of US armed forces for *domestic law enforcement*, the congress, in 1981, made an exception to that act allowing the Department of Defense to get involved in stemming illegal drug traffic. This opened the door for the Department of Defense involvement in other *law enforcement* operations as well. (DoD, 1986, 4)

The military also has indications of this trend. As discussed earlier, the possibilities of military involvement in domestic affairs is captured in the latest military doctrine. Field manual 3-0 separates customary operations other than war scenarios into two fronts: stability operations, which focus on the more customary operations other than war scenarios abroad, and support operations, which focus more on military operations in support of US civil authorities. Although this is not intended as an extension of military purpose doctrine, it is recognition of the Army's changing role on domestic front and of some subsequent changes that are gradually legalizing that area. Civilians are not alone in contesting this change in the Army's role; the following excerpt captures a tone of reluctance from at least one former US Army War College student:

> It would appear that the national security of Engagement and Enlargement has opened the possibility of developing an entangling alliance between military forces oriented on external threats and police force oriented on domestic security and law enforcement by coming closer and closer to crossing the line drawn by the PCA [Posse Comitatus Act]. Routine and recurring military support to civilian law enforcement agencies can involve a gradual assumption of civil roles for the military, which might erode both its apolitical nature and its technical skill. (Diehl 1997, 72)

The debate concerning the Posse Comitatus Act in recent years provides two important conclusions: first, issues surrounding the Army's role in the domestic environment are sensitive, and second, Americans are concerned over potential effects of domestic threats. Both seemed thoroughly entangled and under current trends will continue to cause political friction. Meanwhile, the Army will continue to provide domestic support operations as an instrument of executive powers, just as the legislature will probably continue to debate its further role in homeland defenses.

In either case, if the Army's counterintelligence role does not expand to include other tasks associated with the homeland defense, it must at least provide defenses for its own installations as part of the overall homeland defense. Army installations must resist the effects of threats. Successful attacks on Army installations could increase public fear, erode valuable resources and capabilities, and strengthen the power and resolve of threat groups. Of all the adverse effects, it is public fear that could be affected the most by threat activities against Army installations. As a symbol of American strength and defense, Army installations or government facility or interest present an extremely high symbolic value as a potential target of domestic threat. Accordingly, in every account following a threat strike, the actions taken by the installation commander to prepare

against threats, like those of USS *Cole,* the Federal Building in Oklahoma, and the Pentagon will be publicly scrutinized.

Finally, commanders must address the same questions, at least rhetorically, that William Natter refers to as "accountability to the unreasonable," when Americans ask those accountable for protecting the homeland or protecting their sons and daughters:

> What is being done? What assurances do we have? How much money has been spent? And, perhaps the most significant question, have we as a nation done everything conceivably possible? This last question leaves representatives and senators vulnerable if, heaven forbid, something catastrophic occurs. (Natter, 2000, 232)

A commanders' inherent responsibility to protect the Army installations presents a final area affected by the Posse Comitatus Act. As mentioned earlier, this act does not prevent military law enforcement activities beyond the installation boundaries. But it prevents the military from conducting law enforcement activities in direct support to civil authorities, where civil support is the primary motive for the activity. Whether or not commanders improve security awareness to the full parameters of their areas of interest will depend on their understanding of the provisions established under military purpose doctrine and what they feel is within their inherent authority to defend the installation and areas of interest against domestic threats.

Section II. Conclusions and Recommendations

For the Army, Natter's rhetorical question presents a compelling argument for standardizing its domestic threat doctrine and sorting through the legal implications of conducting counterintelligence within its areas of interest. The first task implies that the Army must provide a standard threat model that will incorporate the full-threat spectrum,

including the most dangerous, as well as the most likely scenarios. The Army must increase emphasis on terrorism.

As mentioned in chapter 4, a standard threat model will ensure that threat analyses across all installations and areas of interest, that subsequent threat reports are standardized, and that resources and crisis response decisions are based on the measurable differences between local circumstances and conditions. A threat model, similar to the one presented in figure 4, will help provide installations and areas of interest with standard metrics to evaluate threat groups and to focus homeland defense operations. It will ensure that a threat score of "seven" at one installation is similarly based and equal to a "seven" at another installation and that both are less serious than a threat receiving a rating of "ten" at still another installation. Likewise, any given installation should characterize one threat group the same as any other installation. This standardization also provides continuity between installation counterintelligence, law enforcement and force protection agencies, and collaboration between the installation and local civil authorities.

To fully answer the question, Have you done everything conceivably possible? the Army must also accomplish the second task (Gilligan 1999, 21). Through its commanders and their staffs, it must provide clear and progressive guidance with regard to conducting counterintelligence, law enforcement, and homeland defense operations within the constraints of legitimate exceptions to the Posse Comitatus Act. To accomplish their inherent responsibility to protect the installation and areas of interest, commanders must receive a view beyond their immediate boundaries; they must be allowed to conduct the necessary counterintelligence to anticipate domestic threats.

Counterintelligence and law enforcement operations stemming from the installation commander's inherent authority to maintain law and order on the installation and areas of interest are permissible. Accordingly, those actions necessary to accomplish those operations are permissible. Even off the installation, "the Military Purpose Doctrine generally will permit . . . actions that support a legitimate military purpose" and "where a legitimate, independent military purpose exists, military law enforcement officials are authorized to conduct activities. Stated differently, when off-post criminal activity adversely impacts the welfare of persons and the efficiency of operations on post, a legitimate, independent military purpose exists" (Gilligan 1999, 21).

To promote but justify homeland defense operation, the Army must provide more definitive guidance on determining the military connection between off-post threats and their adverse impact against installation interests. The DTIM Legal Assessment Model at figure 4, or something similar, could be used to provide a systematic process whereby all essential elements for determining the connection would be considered. Such a model would help standardize homeland defense operations across all CONUS installations and areas of interest and provide many of the same subsequent benefits as the Domestic Threat Assessment Model. A standard legal model would offer two additional benefits: first, it would assist Army counterintelligence and military law enforcement in defining and articulating the military connection behind its activities, and second, it would provide a standard training platform for counterintelligence and military law enforcement personnel. Both benefits might provide a more productive dialogue between law enforcement and installation legal advisors to assist with defining the military connection.

The notion that using these models might provide a common language among installations and areas of interest is a powerful one. It would provide installations and areas of interest the ability to collaborate without diminishing their flexibility to tailor their homeland defense operations to a specific threat or legal environment. This common language could also act as a forum from which to develop or improve doctrine. The model worksheets provide both continuity and a source for further inquiry without the added liability of counterintelligence against specific persons or organizations. Additionally, the model provides a platform that is easily evaluated, which would accommodate additional variables or improvements in metrics and subsequent changes at the strategic and operational levels.

One warning to using these models or any other system, however, is provided by FM 100-19, *Domestic Support Operations*, and should always remain at the top of the installation's DTIM checklist:

> Laws governing use of the military in domestic operations are complex, subtle, and ever-changing. For this reason, commanders should discuss plans, policies, programs, exercises, funding, and operations with their legal advisors. (FM 100-19 1993, 3-1)

Finally, the Army must increase its visibility of crimes, as they pertain to the military purpose doctrine and the installation commander's inherent authority, through the entire adjudication process. Court findings and legal interpretations are continuously building legal precedence with regard to installation force protection and law enforcement. This precedence must be collected, collated, analyzed, and where appropriate, integrated into current security planning and operations and law enforcement. This process should include the same law enforcement, legal, security, and

other functional advisors who are responsible for installation security and who normally sit on the force protection council, but at a minimum, should at least include law enforcement and legal advisors.

DA level officials should develop a formal process to improve its awareness of those changes occurring in the civil and military court systems affecting the other services. For example, a joint committee representing the services could provide insight into the lessons learned through an analysis of their respective appellate court findings or legal interpretations. This information would assist each service because "Congress has enacted statues requiring the military departments to protect military installations and property," and with the exception of the Coast Guard, the Posse Comitatus Act affects all and, certainly, all including the Coast Guard are affected by domestic threat (Gilligan 1999, 21). It would help standardize counterintelligence, law enforcement, and homeland defense procedures DoD-wide, as well as providing the benefits of synergy.

Section III. Future Research

Because homeland defense is a relatively new emerging area, there is much that can be researched to bridge gaps with respect to current doctrine and to establishing some fundamental data to support current processes and recommendations. Consequently, this section discusses those areas where future research might prove productive. This discussion will cover areas starting from more strategic and philosophical recommendations and proceed to those that are more operational and applicable to this thesis.

The first recommendation is to explore the doctrinal similarities and differences in providing counterintelligence, law enforcement, and security measures between stability

operations and domestic operations. It appears that counterintelligence, law enforcement, security, and force protection operations in the domestic environment may parallel those being conducted in support of stability operations. There may not be a defined enemy during stability operations, but there are still adversaries. In such environments aggression takes the form of criminal acts rather than formal enemy operations. This parallels domestic operations in that threats may fall along the threat spectrum from unsophisticated criminals to terrorist. Also this appears to be true in combat operations at the higher end of the operation spectrum. However, in combat operations criminal acts threatening the Army take a back seat to the main effort. But once the theater matures and enemy combat power is reduced, security activities and force protection will probably become increasingly more focused on countering criminal activities similar to the domestic environment.

Another area for future research focuses on more strategic homeland defense-related activities in the joint arena to establish a basis for conducting similar Army homeland defense operations. Here, future research might compare trends between the armed services in three areas: (1) comparative study of law enforcement and homeland, (2) a comprehensive study of appellate court findings and legal interpretations regarding military-civilian enforcement and DTIM, and (3) a study of trends regarding military assistance to civil authorities that is provided as an exception to Posse Comitatus. Each area would provide insight from a broader perspective than the Army alone. Since the services, as discussed earlier, must all provide installation or base protection in the CONUS and since the same laws and similar regulations equally affect them, this

research may provide some collective insight and synergy for developing and improving current systems and processes.

Measuring the accumulative adverse effects of installations from each of the different threat groups is the next area of research focus. This would provide some insight into the effects from the most dangerous versus the most likely threat scenarios. For example, what are the cumulative effects on installations from threat groups that are more pervasive and strike more frequently, such as drug traffickers and gangs, as opposed to the effects on installations from the potentially more dangerous threat groups, such as extremists and terrorists? This research might address a possible oversight in the Army's approach to its threat doctrine. It may even answer questions concerning the probability of a threat group transitioning into more sophisticated threat groups.

Findings from this research might also be used to evaluate the Domestic Threat Assessment Model at figure 4. It could potentially answer some of the following questions: (1) Are the appropriate threat groups included on the list? (2) Is the ranking appropriate for each threat group? And (3) Based on their adverse effects, are the metric weightings assigned to each threat group appropriate?

Correspondingly, future research might directly address the validity and reliability of the Domestic Threat Assessment Model. Research could test these components by evaluating either real criminal data or fabricated scenarios using realistic crime data to determine if the assigned metrics are proportionate to the actual threat. This method would allow a comparison of the model against similar threats to see if scores remain constant or reliable. Finally, this method might bring to light other elements that may not be included in the model, but affect a realistic point assessment.

Testing the validity and reliability of models lends to a final recommendation for future research. The same method recommended for the Domestic Threat Assessment Model could also be used to test the validity and reliability of the DTIM Legal Assessment Model. Researchers could provide scenarios using either real or at least realistic criminal data to validate the model. Methodology would hinge on successful developing a series of scenarios that consist of multiple variables including those listed in the model and any others that are applicable. Research could then test the validity of each variable and its conditions independently. This methodology could confirm or deny the inclusiveness of the current set of variables and conditions. It would also validate the metric system for each variable condition, as well as the reliability by confirming similar scores when tested against similar situations.

Conclusion

The recommendations and conclusions presented in this chapter, as well as those discussed included in the preceding chapters, are by no means inclusive or even definite in nature. They represent only a single view regarding the extremely complex and ever-changing area of homeland defense. This thesis is meant to broaden the current perspective toward conducting homeland defense and homeland defense-related activities and to point out and discuss areas affecting its development. Although the Army can neither predict the changes in law nor the twists and turns presented in case law, it can actively compile, assess, and integrate the current laws, legal exceptions, and subsequent interpretation of those laws by the courts in order to improve homeland defense operations. Whether this endeavor meets the priority threshold in an environment or increasing operations tempo or not, current trends indicate that the potential for domestic

threats against CONUS Army installations is on the rise. Americans and their congressional representatives are concerned about domestic threats and that the inherent responsibility of commanders to protect their installation grows more acute. As a final note, JP 3-09.2 provides the bottom line for initiating improvements in this are: "An effective intelligence and counterintelligence is essential in order to identify the threat" (1998, X).

REFERENCE LIST

Carter, Ashton, John Deutch, and Phillip Zelikow. 1998. Catastrophic Terrorism: Tackling the New Danger. *Foreign Affairs* 77, no 6 (November-December): 80-94.

Chairman of the Joint Chiefs of Staff. 1998a. Chairman of the Joint Chiefs of Staff Instruction 214.01, *Military Support to Foreign Consequence Management Operations.* Washington, DC: Department of Defense.

_____. 1998b. Joint Publication 3.07.2, *Joint Tactics, Techniques, and Procedures for Antiterrorism.* Washington, DC: Department of Defense.

Cohen, William S. 1997. *Report of the Quadrennial Defense Review.* Washington, DC: Department of Defense, March.

_____. 1999. Preparing for a Grave New World. *The Washington Post,* 26 July, A19.

Cordesman, Anthony. 2000. Defending America: Redefining the Conceptual Boarders of Homeland Defense, Home Defense: Coping with the Threat of Indirect, Covert, Terrorist, and Extremist Attacks with Weapons of Mass Destruction (draft). Washington, DC: Center for Strategic and International Studies, 2000.

Cohen, William S. 1999. Preparing for a Grave New World. *The Washington Post,* 26 July, A19.

Defense Special Weapons Agency. 1998. DSWA Publication DSWA-AR-40H, *Weapons of Mass Destruction Terms Handbook.* Alexandria, VA: Defense Special Weapons Agency.

Diel, J. 1997. G. Cop and the Soldier: An Entangling Alliance. The Posse Comitatus Act and the National Security Strategy of Engagement and Enlargement. Carlisle, PA: U.S. Army War College, April.

Ember, Lois R. 1996. FBI Takes Lead In Developing Counterterrorism Effort. *Chemical and Engineering News* 76, no 46 (4 November): 10-18.

Federal Bureau of Investigation. 1998. *Weapons of Mass Destruction Incident Contingency Plan (WMDICP).* Washington, DC: Federal Bureau of Investigation, National Security Division, Domestic Terrorism/Counterterrorism Planning Section.

Frostic, Frederick L. 1997. Quoted in Earl H. Tilford Jr., *National Defense into the 21st Century: Defining the Issue.* Carlisle, PA: U.S. Army War College Strategic Studies Institute.

Gilligan, Matthew J. 1999. Opening the Gate. *Military Law Review* 161 (September): 1-15.

Hoffman, Bruce. 2000. Terrorism by Weapons of Mass Destruction: A Reassessment of the Threat. In *Transnational Threats: Blending Law Enforcement and Military Strategies*, ed. Carolyn W. Pumphrey, 85-104. Carlisle, PA: Strategic Studies Institute, November.

Hoffman, David. 1997. Suitcase Nuclear Weapons Safely Kept, Russian Says. *The Washington Post*, 14 September, A23.

Jackson v. State of Alaska. 1991. 22 Cr L 2338 (AL).

Jackson, Mark A. 2001. *Domestic Threat Intelligence Management.* Fort Leavenworth, KS: Command and General Staff College.

Larson, Eric V., and John E. Peters. 1999. The Army Role in Homeland Defense: Concepts, Issues and Options (Draft). RAND Arroyo Center, October, vi-xvii.

Larson, William Jed. 1997. Chemical and Biological Weapons: A Growing Problem for the CINC. Thesis, Naval War College.

Lujan, Thomas R. 1996. *Legal Aspects of Domestic Employment of the Army.* Carlisle Barracks, PA: Strategic Studies Institute, U.S. Army War College.

Maze, Rick. 1995. Military a Step Closer to Domestic Terrorism Battle. *Navy Times* 44, no. 37 (19 June): 9.

O'Hanlon, Michael. 2000. Rethinking Two War Strategies. *Joint Force Quarterly*, spring, 11-17.

People v. Burden. 1979. 94 MI App 209, 288 NW2d 392, revd (411 MI 1981) 56, 303 NW2d 444.

Peters, John E. 2001. Preparing the U.S. Army for Homeland Security: Concepts, Issues, and Options. Santa Monica, CA: RAND.

Pumphrey, Carol W. 2000. Transnational Threats: Blending Law Enforcement and Military Strategies. Washington, DC: Strategic Studies Institute.

Riley v. Newton. 1996. 94 F3d 632, 10 FLW Fed C 349 (CA11 GA).

Rumsfeld, Donald H. 1998. *The Report of the Commission to Assess the Ballistic Missile Threat to the United States.* Washington, DC, July 15, 8-9.

State v. Harker. 1983. 663 P2d 932, 936 (AK).

State v. Nelson. 1980. 298 NC 573 (1979NC), 260 SE2d 629, cer den, 446 US 929, 64 L Ed 2d 282, 100 S Ct 1867.

State v. Tureblood. 1980. 541, 265 SE2d 662 (NC).

US Department of State. 2000. Department of State Publication 10687. Patterns of Global Terrorism 1999. Washington, DC, April. Database on-line. Available from http://www.state.gov/www/global/terrorism/1999report/ 1999index.html. Internet. Accessed on15 January 2002.

United States v. Bacon. 1988. 851 F2d 1312 (CA11 GA).

United States v. Brown. 1980. 9 NJ 666 (JN 1980).

United States v. Del Prado-Montero. 1984. 740 F2d 113 (Puerto Rico 1984), cert den 469 US 1021.

United States v. Hutchings. 1997. 127 F3d 1255, 97 Col J C A R 2426 (CA 10 UT 1).

United States v. Red Feather. 1975. 392 F Supp 916 (CD SD).

United States v. Strouder. 1989. 724 F Supp 951 (MD GA).

United States v. Walden. 1974. 590 F2d 372 (CA4 VA).

US Army. Deputy Chief of Staff of Operations. 2000. Homeland Security (HMS) Army Strategic Plan, Initial Distribution, Draft, 18 October.

_____. Training and Doctrine Command. 1999. *Supporting Homeland Defense.* White Paper, May. Document on line. Available from http://www.fas.org/ spp/ starwars/program/homeland/final-white-paper.htm. Internet. Accessed on 15 January 2002.

US Congress. Senate. 2000. Oversight Subcommittee of the House Transportation Committee. *U.S. Representative Tiller Fowler (R-FL) Holds Hearing on Terrorist Defense.* 106th Congress, 2nd Session, 6 April.

US Department of the Army. 1977. Regulation 210-10 *Installation Administration.* Washington, DC: Department of the Army.

_____. 1978a. Regulation 190-13, Physical Security: *The Physical Security Program.* Washington, DC: Department of the Army.

_____. 1978b. Regulation 190-30, *Military Police Investigation.* Washington, DC: Department of the Army.

_____. 1983. Regulation 500-51, *Support to Civilian Law Enforcement.* Washington, DC: Department of the Army.

_____. 1985. Regulation 195-2, *Criminal Investigation Activities.* Fort Belvoir, VA: USACIDC.

_____. 1987. Field Manual 1910, *Law Enforcement Operations.* Washington, DC: Department of the Army.

_____. 1993a. Field Manual 100-5, *Operations.* Washington, DC: Department of the Army.

_____. 1993b. Field Manual 100-19 (Fleet Marine Force Manual 7-10). *Domestic Support Operations.* Washington, DC: Department of the Army.

_____. 1994. Field Manual 100-23, *Peace Operations.* Washington, DC: Department of the Army.

_____. 2000a. U.S. Army Command and General Staff College, *National Military Strategy.* Fort Leavenworth, KS: USACGSC, August.

_____. 2000c. U.S. Army Criminal Investigation Command Operations Memorandum 002-00, *Force Protection Initiatives and Domestic Threat intelligence Management.* Fort Belvoir, VA: USACIDC, February.

_____. 2001. Field Manual 3-0, *Operations.* Washington, DC: Department of the Army.

US Department of Defense. 1986. U.S. Department of Defense Directive 5525.5 *Cooperation with Civilian Law Enforcement Officials.* Washington, DC: Department of Defense.

_____. 1987. Inspector General Policy Memorandum, *Criminal Drug Investigative Activities.* Washington, DC: Department of Defense, 1 October.

_____. 1991. U.S. Department of Defense Directive 5200.8. *Security of Military Installations.* Washington, DC: Department of Defense.

_____. 1994. Department of Defense Directive 3025, *Military Assistance for Civil Disturbance.* Washington, DC: Department of Defense.

Utgoff, Victor. 1999. Bruce Hoffman's View of Terrorism by Weapons of Mass Destruction: Another Perspective.

The White House. 1999. *A National Security Strategy for a New Century.* Washington, DC: The White House, December.

Zoellick, Robert B. 2000. A Republican Foreign Policy. *Foreign Affairs*, January-February ,45-70.

INITIAL DISTRIBUTION LIST

Combined Arms Research Library
US Army Command and General Staff College
250 Gibbon Ave.
Fort Leavenworth, KS 66027-2314

Defense Technical Information Center/OCA
8725 John J. Kingman Rd., Suite 944
Fort Belvoir, VA 22060-6218

MAJ Douglas Horton
DLRO
USACGSC
1 Reynolds Ave.
Fort Leavenworth, KS 66027-1352

LTC Clay Easterling
DJMO
USACGSC
1 Reynolds Ave.
Fort Leavenworth, KS 66027-1352

LtCol Rick Messer
DJMO
USACGSC
1 Reynolds Ave.
Fort Leavenworth, KS 66027-1352

MAJ (P) Kenneth D. Plowman
12 Little Creed Crt.
San Ramon, CA 904583-1815

CERTIFICATION FOR MMAS DISTRIBUTION STATEMENT

1. Certification Date: 31 May 2002

2. Thesis Author: MAJ Frederick L. Washington

3. Thesis Title: The Army's Counterintelligence Role in Homeland Defense

4. Thesis Committee Members _____

Signatures: _____

_____

5. Distribution Statement: See distribution statements A-X on reverse, then circle appropriate distribution statement letter code below:

A B C D E F X SEE EXPLANATION OF CODES ON REVERSE

If your thesis does not fit into any of the above categories or is classified, you must coordinate with the classified section at CARL.

6. Justification: Justification is required for any distribution other than described in Distribution Statement A. All or part of a thesis may justify distribution limitation. See limitation justification statements 1-10 on reverse, then list, below, the statement(s) that applies (apply) to your thesis and corresponding chapters/sections and pages. Follow sample format shown below:

EXAMPLE

Limitation Justification Statement	/	Chapter/Section	/	Page(s)
Direct Military Support (10)	/	Chapter 3	/	12
Critical Technology (3)	/	Section 4	/	31
Administrative Operational Use (7)	/	Chapter 2	/	13-32

Fill in limitation justification for your thesis below:

Limitation Justification Statement	/	Chapter/Section	/	Page(s)
	/		/	
	/		/	
	/		/	
	/		/	
	/		/	

7. MMAS Thesis Author's Signature: _____

STATEMENT A: Approved for public release; distribution is unlimited. (Documents with this statement may be made available or sold to the general public and foreign nationals).

STATEMENT B: Distribution authorized to U.S. Government agencies only (insert reason and date ON REVERSE OF THIS FORM). Currently used reasons for imposing this statement include the following:

1. Foreign Government Information. Protection of foreign information.

2. Proprietary Information. Protection of proprietary information not owned by the U.S. Government.

3. Critical Technology. Protection and control of critical technology including technical data with potential military application.

4. Test and Evaluation. Protection of test and evaluation of commercial production or military hardware.

5. Contractor Performance Evaluation. Protection of information involving contractor performance evaluation.

6. Premature Dissemination. Protection of information involving systems or hardware from premature dissemination.

7. Administrative/Operational Use. Protection of information restricted to official use or for administrative or operational purposes.

8. Software Documentation. Protection of software documentation - release only in accordance with the provisions of DoD Instruction 7930.2.

9. Specific Authority. Protection of information required by a specific authority.

10. Direct Military Support. To protect export-controlled technical data of such military significance that release for purposes other than direct support of DoD-approved activities may jeopardize a U.S. military advantage.

STATEMENT C: Distribution authorized to U.S. Government agencies and their contractors: (REASON AND DATE). Currently most used reasons are 1, 3, 7, 8, and 9 above.

STATEMENT D: Distribution authorized to DoD and U.S. DoD contractors only; (REASON AND DATE). Currently most reasons are 1, 3, 7, 8, and 9 above.

STATEMENT E: Distribution authorized to DoD only; (REASON AND DATE). Currently most used reasons are 1, 2, 3, 4, 5, 6, 7, 8, 9, and 10.

STATEMENT F: Further dissemination only as directed by (controlling DoD office and date), or higher DoD authority. Used when the DoD originator determines that information is subject to special dissemination limitation specified by paragraph 4-505, DoD 5200.1-R.

STATEMENT X: Distribution authorized to U.S. Government agencies and private individuals of enterprises eligible to obtain export-controlled technical data in accordance with DoD Directive 5230.25; (date). Controlling DoD office is (insert).